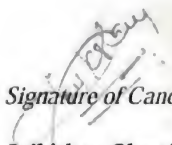
ABSTRACT

Authentication is a kind of System's services and resources verification, authorization as per requirements of the user .It also ensures that the controls over the system and its resources are not illegally obtained by any non-genuine users. Alphanumeric Passwords authentication system is one of the weakest mechanisms currently present with us. There are many scheme totally based on the encryptions and decryptions techniques end to end which has been developed to solve the problems of unauthorized access of system resources but none of them have been proven to be convenient and complex which can secure the system. It has been observed that previous methods are vulnerable to various kinds attack and they are neither user-friendly nor efficient. They are neither user-friendly nor efficient. In this Paper, we have developed a two algorithms for securing password over any channel either over secure or on unsecure channel even it is hacked or known by any person .Even after getting users identifiers like ids and passwords he/she unable to authenticate him/herself and is totally based on time basically called 4D and one way - hash function and another is for securing OTP and Reset code at client side.

DECLARATION

I hereby declare that the research work reported in the dissertation entitled "OPTIMIZATION AND ENHANCEMENT OF AUTHENTICATION PROCESS" in partial fulfilment of the requirement for the award of Degree for Master of Technology in Computer Science and Engineering at Lovely Professional University, Phagwara, Punjab is an authentic work carried out under supervision of my research supervisor Mr. Nitin Umesh Dubey. I have not submitted this work elsewhere for any degree or diploma.

I understand that the work presented herewith is in direct compliance with Lovely Professional University's Policy on plagiarism, intellectual property rights, and highest standards of moral and ethical conduct. Therefore, to the best of my knowledge, the content of this dissertation represents authentic and honest research effort conducted, in its entirety, by me. I am fully responsible for the contents of my dissertation work.



Signature of Candidate

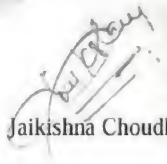
Jaikishna Choudhary

R.No 11100403

ACKNOWLEDGEMENT

I would like to thank the Lovely Professional University, Phagwara Punjab and take the opportunity to work on the Project as a part of the M-Tech. Many people have influenced the shape and content of this project and supported me through it. I express my sincere gratitude to "Mr.Nitin Umesh Dubey" who lighten my path on each and every step. He has been an inspiration and role model for this topic. His guidance and active support has made it possible to complete the research. I also would like to thanks "Mrs.Jasmine Choudhary" and my friends who have helped and encouraged me throughout the working of the project.

Last, but not the least I would like to thank the almighty for always helping me. Finally, I take this opportunity to acknowledge the services to everyone who collaborated in producing this work.



Jaikishna Choudhary

TABLE OF CONTENTS

List of Acronyms / Abbreviations

TLS/SSL	: Transport Layer Security/ Secure Sockets Layer.
MAC	: Media Access Control.
DNA	: Deoxyribonucleic Acid.
PIN	: Personal Identification Number.
OTP	: One Time Password.
API	: Application Programming Interface
USB	: Universal Serial Bus
RFID	: Radio Frequency Identification
ATM	: Automated Teller Machine
CIA	: Central Intelligence Agency
SMS	: Short Message Service
HMAC	: Hash Message Authentication Code
IP	: Internet Protocol

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION

1.1. AUTHENTICATION

Authentication is one of the critical component of many applications, hardware larger and small .It is very challenging task to implement the authentication system while choosing where to authentication is needed, what types of system is needed .It must be safely deployed. It is basically the act of creating the link between the system and the user over secure channel using a perfect identity of the user. The identity could be anything, numbers including; system, people, applications, and message etc. The basic reason to verify the identity are for the following reasons [13]:

- To assure that the piece of information is genuine.
- To create a trust between the multiple parties to whom we interact digitally.
- To get the control access to the system or the resources.
- To get or to bind some sensitive data to an individual, such as encryption etc.

There are various types of authentication technique like:

- Cryptographic Authentication
- Multi-Factor Authentication.
- Single, basic factor Authentication.

These above mention Authentication scheme can be apply on all types of entities that require authentication: Users, System, message, Application etc.

Basic Authentication: It is very commonly used term that the most of the people probably understand already. It commonly called the password based authentication. Passwords is a kind of information that is used to verify the identity of the users. Some of the common examples that falls in this types are:

- The common passwords.
- Host or the system names.
- Applications names.
- Numerical IDs.

It entails the validation of the single credential's pairs- user's identity references and password authentication. This process typically receive the passwords and compare it with the stored data in the database. Following are the benefits of such types of scheme:

- It is easy to manage.
- It is easy to implements
- It is easy for end user to use.

There are some important points for every developers to be aware when using this scheme some of they are pointed below [14]:

- Identifiers like ids and passwords are commonly weakly specified.
- Identities might be spoofed and impersonated.
- Passwords could be susceptible to theft.
- It can be very difficult to scale up and scale down across the distributed computing environment [16].

The Basic authentication is often found to be transmitting of identifiers over a networks could be easily stolen and compromised. We have found some best ways to increase the strength of this scheme:

- By using the digest authentication- Hash and encryption of the identifiers.
- By using the pass phrases and set minimum lengths.
- Force use of alpha numeric symbol passwords with special characters.
- By not storing the passwords in the plain text in the database.
- Implementations of TLS/SSL security mechanism.

Multi-Factors Authentication [2, 18]: It is kind of authentication that uses the combinations of the authentication methods to validate the identity and allocate the resource to the user. It works the most commonly used descriptions of that information which is known by the person, combined with the something in his or her possessions. These are typically:

- The users name and the passwords.
- Tokens

As the security components are layered, the complexity of the system also rise and parts of these it provides the following additional benefits:

- Easy to implements.

- Difficult to spoof or impersonate.

Some the disadvantages of this types of scheme are:

- Deployment can be difficult.
- Token can easily be stolen.
- The management of the scheme can be challenging and especially in the event of the lost or stolen of the tokens.

Cryptographic Authentication [11, 20]: By its name it is clear that it uses the mechanism of cryptography. This types of the technique provides the security in form loss of Confidentialities. Such types of authentication scheme includes the following forms:

- Public key Authentication: This types of authentication occurs when the owners of the key pairs try to communicate with the public keys to authenticate the third parties .there are some methods for public key authentication like the use of the public key itself and the public key certificates etc.
- Digital signatures: It is a kind of puzzle cryptographic. Digital signatures is generated using the owner key pairs and it uses private key to sing the message. Further the signature can be verified only by the corresponding keys.
- Message Authentication code: It uses the Mac .In this method, message authentication code is generated when secrete key is used to with the combinations of information which to be proved authentic. Hashing Algorithms or symmetric encryption is use to generate the MAC and MACs provide the integrity and authenticity.
- Passwords combinations and permutations:

In this Present Era, securing the private data, files, transections are the main task of the technology. But still they have been accessed by the intruders or any person who are not unauthorized to access them. Many system are been hacked easily due to lack of proper algorithms or loopholes in it. Authenticating is the way of confirming the reality and truth of the person who is gaining access to secure data either over channel or any system. Therefore we can say that Authentication means actually confirming the identity of the person .In fact, authentication involves in verifying the validity of any form of the identification. The process of the authentication are basically divided into 3 categories and

are based on what are known for the factors of authentication. And every authentication factors covers a wide range of elements which are used to authentication or verify the person reality and identity to grant the access and approve them for the transection request or accessing the secure data of the system.

In previous password authentication scheme[12][13][14][15], every user has an identifier (user_id) and a password (User password).when user wants to access the remote services he/she has to authenticate him/herself to the remote server, he/she has to fed his/her user_id and User _password to the server. A light authentication method is to store and manage a password table including users_id and users passwords in the remote database of the server. Upon getting user's id and Passwords, the remote server starts matching the user id and users password in the table. Once the user id and user password match the respective data it granted access to the server's facilities to the users. Since the user's password is not encrypted and is stored in the form of plain-text in the table, this scheme is vulnerable. An intruder can imitate a legal user by robbing the user's id and user password from the table. The big disadvantages of this approach is when any intruders intercepts the user id and password from the internet it can reply it later to login , this kind of attack is called reply attack . To avoid the identifiers table from being stolen by intruders, they are generally hashed or encrypted. But during the Transmission it could be stolen by wiretap or by any mean, if any person able to fetch the password he/she can easily get control over the system. Many Research has developed the way for the Positive authentication with three class of elements and are as follows:

- The Knowledge Factors : Like Passwords, Pass Phrase or PIN.
- The Ownership Factors : ID cards, Tokens, Cell Phone.
- The Inherence Factorss : Fingerprint, Retinal Patterns, DNA etc.

To prevent such problems, One-Time Password using one way hash function is developed. But later it has be observed that OTP is also not safe as they are vulnerable at client side. If any person get access to the OTP form the client it can easily initiate the authentication process and bypass the security layers easily.

1.2. FACTORS

The Authentication is based on basically 3 factors and that are as follows:

- Something's that user has,
- Something's that user knows and
- Something's the user is.

In the very 1st factor, authentication is done by help of any physical devices that an individual has. Device can be token or any smart cards. The person should use this device to the authorizing center to validate and access to the resources. In 2nd factor, authentication is done by the help of something that the person knows like a password or a pass phrases. The person should fed the correct input password or phrase to access to the resources. In 3rd factor, authentication done by help of the physical features of a persons like the fingerprint or the face etc. Nowadays, Basically the Text Based passwords are used for authenticating the user and it is little hard and huge to memorize for long time. Such types passwords are has also vulnerable to many attacks. For example Dictionary Attack, Brute Force Attack and Password Guessing and Key loggers are the well know factor to get the text based password [6, 23]. This is the main disadvantages of the text based passwords. Even Image based password are vulnerable to many attacks. If we are able to get the image of a person in any forms like hard copy of soft copy, we can access to his/her account easily. Similar case in Biometric [18]; like fingerprints. For instance, Apple has introduced the fingerprint passwords locks to its series of iPhones 5c and it was hacked. To Recover the such Damages and makes the authentication harder , the Researchers has developed the graphical based authentications .Since image based password are easy and competitively more light the text based passwords to memorize. The graphical based password schemes which currently exist that are divided into three group [2,3]:

- Recognition of pass-images.
- Repeating actions in a sequential order.
- Reproduce a particular drawing.

But what if, the image is stole from the Database? Intruders again can easily authenticated and access to the resources. Perhaps all such techniques are not secure and assure the safety of the files, data, and transection over any channel.

1.3. TRADITIONAL AUTHENTICATION METHODS

1.3.1. Text based authentication

The password based authentication is the based on Text and it's consist of either alphabet or alphanumeric character even a numbers too. Such types of keys are created at the time of registration .Further user can either reset it or change it. This is most the most common types of techniques used globally by the user or by any company.

Loopholes

The text based authentication can be broken by the following.

Guessing Attack: A password guessing attack is a kind of attack or method of gaining unauthorized access to a computer system or its resource by using a computers and large of words. In this type of attack intruders try to guess the passwords randomly. It is one of the weakest types of known attack in the computer system. For each guess, the probability of getting the authorization is just 1/total no of possible combinations of the digits. For example if any system using 4 digit passwords than there will be total 3844 possible combinations. For each type we guess the passwords, the probably of getting passwords is 1/3844.This attack is similar to Brute force attack but the main difference in both of them is that one is done manually and another with the help of computer system. Social engineering is also done the get the credentials of the users.

1) Dictionary attack: In cryptanalysis, a dictionary attack is one the most used technique for defeating a cipher or authentication mechanism by trying a various decryption key or passwords as much as possible. Such combination are listed and dictionary is formed and they cryptanalysis is done to get access to the system and its resources. We can get various types of software and tools for the same such as Brutus, Cain and Abel, Crack, Aircrack-ng,John the ripper, Airodump-ng,L0phtcrack , Matasploit project , Ophcrack etc. It is very much similar to Brute Force attack But the main difference between both of them is that one has finite list of possible combinations of passwords i.e. dictionary

attack and another has about to infinite list of possible passwords dictionary i.e. Brute Force Attack.

2) Key-logger Attack [29]: Key Logger is often referred as key logging or capturing the keystroke of pressed keywords and recording the action .Since the person using the keyboard is unaware about the attack and the mechanism of it and become the victims and his credentials are compromised. Such types of attack is are basically done to get the bank account details. Key loggers can also be used for understanding the human behaviors for the acoustic analysis is done. Key loggers can be Hypervisor Based, Kernel Based, API-Based, From Grabbing Based, Memory Injection Based, Hardware Based etc.

1.3.2. Token based authentication

In the types of Authentication system, the system is based on the token or a smart cards .The user has to provide the token to the access center for the Authentication. It is not as common as Text based authentication.

Loopholes

The Token based Authentication can be broken by the following.

1) Man in the middle Attack: In cryptanalysis or cryptography, a Man in Middle attack is very common types attack. In this types of attack, intrudes possibly alters the communications and secretly capture the keys and alters the keys between the parties and pretends himself to be a genuine. The best example of Man in Middle attack is eavesdropping. There is a loss of confidentiality in this types of attack. TLS has been developed to avoid such kind of attack.
2) Loss of Token: Security token may be a physical device like USB token or software generated token, virtual token etc. There are basically used for the authentication to the system. Security token are used to prove ones identity electronically. They store cryptographic keys such as digital signature or biometric data such as fingerprints minutiae etc. Some of them are design a tempered resistant and water proof while other may include small keypads to allow the entry of pin or simple bottoms to starts generation the routine with some display .Special design token may include USB connector or RFID

functions or Bluetooth wireless interface. In case if such security token are lost or cloned then it will create a big security loopholes. There are some vulnerabilities like loss and theft, Attacking, Breach of Codes etc.

1.3.3. Biometric authentication.

It uses the basic Human Natural Physical Features and such features don't change throughout the life time such as Fingerprints, retina etc. [18, 20, 29] .During the Registration such features are fed into the database and further used for the verification and access the resources[35, 36].

Table 1.1.Examples of Biometric.

Biometric	Acquisition Devices	Sample	Features
Iris	Infrared-Enable camera , Pc camera	Black and white iris image	Furrows and striations of iris
Voice	Microphone, telephone	Voice Recording	Frequency , Vocal patterns and cadence
Signature	Signature tablets, Motion–sensitive Stylus	Image of signature and record of related dynamic measurement	Stroke, speed, pressure and appearance of signature
Face	Image camera , PC camera , video camera	Optical and thermal image of face	Relative shape and position of nose , position of cheek bones
Hand	Proprietary Wall mounted unit	3-D images of sides and top of the hands	Height and width of bones and joints present in the fingers
Retina	Proprietary desktop or Wall mounted unit	Retina Image	Blood vessels patterns and retina

Fingerprint	Desktops peripherals device, Pc cards, Mouse chip or reader embedded in keyboard	Fingerprint image (silicon , optical , ultrasound or touch less)	Location and direction ridge endings and bifurcations on fingerprints, minutiae

Loopholes

The Biometric based Authentication cracked by the following:

1) False-positive matches and false-negative matches: False positive is an error in data result in which a test result improperly indicate the presences of condition. While false negative is an error in which a test result improperly indicate no presences.
2) Replay attack [23]: It is also known as playback attack. Packets are captured by the intruders in the middle of the transmission of data and resend by them to gain access or control over the system. Such types of attacks are very much famous in banking sectors. To avoid such types of attack Session tokens are used. We can also use hash function. Token session should be chosen by the help of random process. It is also called a pseudorandom process. One time Passwords can also prevent such types of attack [10,37].
3) Altering the biometric representation of features: Biometrics include all the hardware, software and interconnecting end to end which enable the biometric process. These days our face, iris, DNA Profile become digital file and these files becomes very difficult to protect. Recent studies on biometrics states that these files can easily be stolen without any great efforts. It's easy to replace the swiped card and extract the data and identifies from the card [34, 30,35,36].

1.3.4. Graphical based authentication.

It is a kind authentication system which works on the users selected images in a predefined order and is presented in the graphical user interface. For this reason

this approach is called graphical user authentication system. It is very much easier than the text based passwords system .It offers the better security then the text based password system. If there are 100 images passwords, there are about 100^8 possible combination and it could take about millions of years to break at the average delay of 0.1 sec. In this method, the graphics images are used since it is easy to remember the image then a plain text. Because of this reason this methods is competitively high demand in the market .Due to this good features in the system, it ignores the cracking of the system by either brute-force, dictionary or any key logger attack.

Loopholes

1) It is most difficult to hack the system that is protected by the system .but if the database is hacked then it might increases the chances to access the data. Shoulder surfing attack is one the best known attack for the scheme. It is a kind of technique in which attacker observes someone shoulder to get the information. Shoulder surfing is an effective way to get the sensitive information in crowed place because it relatively easy to stands next to the someone and watch as they fill the forms , pin of at an ATM machine or graphical pictures during the logging.

1.4. SOME OF THE COMMON ATTACKS [6, 7, 23, 24, 29]:

Table 1.2: Attack Summary

Attack	Security Problems	Pervasiveness	Attack Descriptions
Keystroke Confusion	Masquerade as someone else	Obsolete	The is a bug that can be found in the software time sharing which allow a peculiar sequence of character to skip password checking
Trojan horse	It recovers the hidden information.	Most common, innovative	It pretends to be original script and

			bypass along with the genuine software to the system
Password Audit	It also recovers the user passwords	Common	It review the audit of the records of users mistakes while logging
On-line password guessing	It also recovers the user passwords	Trivial	Try to guess the passwords.
File theft of the passwords	It recovers all the users passwords	Obsolete	Lack of high security in the database allow intruders to steal he files.
Bogus password change	It recovers user's password	Trivial	Intruders convinces victim to change their passwords to a word selected by them
Shoulder surfing	It recovers user's password	Common	Intruders watches a user passwords standing behind.
Keystroke sniffing	It recovers user's password	Common	Software log the key pressed by the user.
Trojan login	It recovers user's password	Common	It mimics the stander logging system.

1.5 ELEMENTS OF AN AUTHENTICATION SYSTEM

We must considered the several elements:

1. The 1st elements include : Person, entity and principal which denotes the certain group of people.
2. The 2nd elements include : The different characteristics between certain people and groups.
3. The 3rd elements include : The administrator who manage the database and authorize and differentiate certain group or certain people from other people.
4. The 4th elements include : It act as magical device which could respond to words, numbers.
5. The 5th Elements include : The administrator grant the services if identity is verified and access the control mechanism. If the authentication process then users are not allowed to access the system or resources.

Table 1.3. Example of the five elements in authentication system.

Authentication element	Cave of the 60 thieves	Password Login	Machine (Teller)	Web server to client
Person, Entity, Principal	Any person who knew the credentials like password	Authorized user	Owner of any bank account	Web site to client
Distinguishing characteristic, authenticator n tokens.	Password "open, sesame"	Secrete passwords	ATM card and PIN	Certificate with public key

Owners, Administrator, System owner	The 60 thieves	Enterprise owing system	Bank	Certificate authority
Authentication Mechanism	Device(Magical) which respond to the words	Validation software for passwords	Validation software for card	Validation software for certificates
Authentication element	Cave of 60 thieves	Password login	Teller Machine	Web server to client
Access control mechanism	Process to roll the stone from in front of the cave	Login process , access control	Allow transections	Marks the page as secure (Brower)

CHAPTER 2: REVIEW OF LITERATURES

2.1 LITERATURES SURVEY

The literature review is one the basic and compulsory task which serve as the base of the research. During this phase article, published papers, books, news, newspapers from internet and internal document of any related thesis regarding the same field has been analyzed. We can only two choice when we deals with the research approach; quantitative or qualitative. Both are equally importance but is basically based on the fundamental values on which the research are going to be conducted. The main goal of qualitative is to get the deeper and internal understanding of the existing problems and the situation. We have studied some papers and theirs descriptions are as described below.

- I-En Liao, Cheng-Chi Lee, and Min-Shiang Hwang. A password authentication Scheme over insecure networks, Journal of Computer and System Sciences 72 (2006), no.4727–740. [13].

In this paper, the basic technique of Authentication is discovered. Over unsecure networks for the smart card.

1. The advantages of algorithms are as follows:
2. Users can easily generate and modify their pass text
3. The confirmation of the table or pass text database is not stored somewhere else.
4. It has **One-time password seniority**, which gets changes for every transaction.
5. The precaution is totally established on both properties i.e. hashing function and the discrete logarithm.
6. There are the provision of the Mutual authentication between the server and the user. It can withstand with reply and guessing attack. Table of verification of password is not stored in the database.

Problems: Secretes key stored in the database. If the key is exposed the system can easily be destroyed. If the password is comprised, the system can be destroyed. If the OTP is compromised, the system can be destroyed.

- Dr.AnanthiShesashaayee, D. Sumathy Associate Professor & Head, Department of Computer Science, Quaid E Millath Government College for Women, Chennai, Tamil Nadu, India Research Scholar, Department of Computer Science, Quaid E MillathGovernment College for Women, Chennai,Tamil Nadu, OTP Encryption Techniques in Mobile for Authentication and Transaction Security.India.IJIRCCE ISSN(2320- 9801,2320-9798)-2014 [1].

The proposed system developed to secure the OTP using Feistal Networks. Encryption and Decryption technique is used. Here the user PIN act as Key which is further required to decrypt the OTP. Here in the system again the threats exist. Again the problems is with the OTP. The system defined that the OTP is send to the user mobile or the email. But it doesn't deals with the solution if the cell phone is lost or stolen, the One Time Password can be misused by the attackers for the handling the transection or login in to the system. Pin is of 4 digit which can be cracked less than in a days with the latest super computer.

- M Viju Prakash, P Alwin Infant, and S Jeya Shobana. Eliminating vulnerable attacks using one time password and pass text analytical study of blended schema. Universal Journal of Computer Science and Engineering Technology, 1(2):133–140, 2010. [7]

The Algorithms is explained below:

1. The user verify himself to SP by the help of credentials which is known to SP.
2. When the user needs to trigger his cell phone for the OTP accepter, SP forwards the user's gateway to SE in URL which have an activation request and a Secure Object.
3. SE confirms the Secure Object which arrive from SP, and gets the cell phone details and number and might be other unique identification number
4. It generates an activation code and send to the client system and an SMS to the cell phone demanding to start the client software. The cell phone pop up the client asking to fed the activation code, available on his PC, and transfer the code to SE.
5. SE confirms the code which is same send to the PC, and ask for encryption and decryption of the code send to the mobile
6. The client select a personal identification number (PIN) and fed it on the cell phone. And further the work is carried out.

Problems: This is also not a secure algorithms for the verification. Again the problems arise if the OTP is compromised or mobile is lost or the reset code that is send to the email is hacked. Each and every research deal with the mechanism for protecting the passwords in the physical layer , and presentation layer but none of the scheme deals to add the security features if passwords or OPT is compromised.

• Brajesh Kumar Kushwaha . An approach for user authentication one time password (Numeric and graphical) scheme. Journal of Global Research in Computer Science, 3(11), 2012. [3]

In this algorithms, the OTP and graphics pictures are used to validate the user and authorize the resources to the user. Here OTP is generated using Algorithms and Graphics are kept constants for the each phase. During the Authentication again the Opt is send to the mobile which is totally unsecure if compromised.

Note: Here and every algorithms deals with generation of the OTP but none the papers deals with the protection and securing the OTP. In each and every case, if the mobile is lost or stolen, it can create a huge problems for the genuine user. It is vulnerable to shoulder attack. People standing behind can easily see the graphical picture that user selects during the authentication.

• Vaidya, Binod, Park, Jong Hyuk, Yeo, Sang-Soo & Rodrigues, Joel JPC (2011) [5]. Robust one-time password authentication scheme using smart card for home network environment. Computer Communications, 34, 326-336.[5]

Following problems exist with this prosed scheme:

It has been seem that the proposed scheme required more computational cost. Inefficient if password is compromised. System can be destroyed No security measures taken at end user side.OTP is not secure at user side.

• John G Brainard, Burton S Kaliski Jr, and Ronald L Rivest. Method and apparatus for Performing enhanced time-based authentication, April 22 2008. US Patent 7,363,494.[10]

The deals with the mechanism for generating an authentication code combined with an entity, the steps as follow:

1. Fetching a secret stored key combined with an entity.

2. Calculating a dynamic value related with a time interval. Recover a first generation value expressive of a number of previous authentication code which is developed at that time interval and then after PIN is received. Then after a new code is generated by the combinations of dynamic values, PIN and secrete code for a certain interval of time. Then second value is generated with to compare with the receipt of PIN.

- Fabian Monrose, Michael K Reiter, and Susanne Wetzel. Password hardening based on keystroke dynamics. International Journal of Information Security, 1(2):69–83, 2002. [25].

This paper represent the novel technique for improving the security of the passwords. The papers basically deals with generation of patterns of user key stroke and further the key patterns is developed with the keys stroke of the user id and passwords .From the patterns the hardened passwords is developed and stored. Further the used for the authentication to the system. During verification the keystroke and patterns are compared. The main problems associated with the scheme is that if the ids and passwords are compromised, after a little efforts we can easily verify our self to the system.

- Ting-Yi Chang, Cheng-Jung Tsai, and Jyun-Hao Lin. A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices. Journal of Systems and Software, 85(5):1157–1165, 2012.[2]

This paper proposes a new methods of graphical-based password KDA system. It deals with the pressure features and keystroke dynamics. The pressure of touch and typing patters and images is stored .During the verification the user's needs to apply the same pressure and type passwords within the same sequence on the touch screen and choose the respective image which he register at initial stage. It seems to be very complex. Here involves 3-tire phase which is little hard to memorize.

- TongLiang Li and ZhiGang Jin. A new low cost one time id and password authentication protocol using popular removable storage devices. In 2009 Second International Conference on Intelligent Networks and Intelligent Systems, pages 213–216.IEEE, 2009.[8]

In this methods, plain text is not transferred over the network, by the use of hash function the data are protected at the both of the ends. The author deals with securing the

user and server from the most common attacks. Furthermore, the concept of random numbers are used and the server and the end user or client exchange two random numbers which is further use to generate a session id key after authentication. Different types of technique are used for generating the key this proposed scheme. By the help of the new proposed methods, the user can easily "memorize" a random number which is the part user's and user's password. Thus is makes the scheme as a one-time ID and one-time password along with the protection of user identity. This scheme also support Mutual authentication, which makes the scheme with the ability of principal aliveness and message freshness.

- Blake Ross, Collin Jackson, Nick Miyake, Dan Boneh, and John C Mitchell, Stronger Password authentication using browser extensions. Usenix security, Baltimore, MD, USA, 2005, pp. 17–32. [17]

The Authors proposed an extension for browser, password hashing and develop methods to boost the password authentication on the web or at server side with minimum change to the user experience and no change to current configuration of the server. The main purpose of the paper discusses the direct types of challenges while deploying Password Hashing in a browser. Further, they discuss a methods to get rid of scripts attack on sites which are phished. Theirs scheme enables users to securely enter their credentials within the browser.

- Francesco Bergadano, Daniele Gunetti, and Claudia Picardi. User authentication through keystroke dynamics. ACM Transactions on Information and System Security (TISSEC), 5(4):367–397, 2002. [26]

In this paper Authors present an actual measurement of the keystroke dynamic which bound the uncertainty of biometric feature. The have tested theirs technique on 154 individuals and achieved the False Alarm Rate which is about 4% and the pretender Pass Rate which is less than 0.01%. Theirs execution is reached using the same sampling of keywords for each and every the entity and individual, by allowing error in typing , without any particular adaptation for the authentication system with respect to the available group of typing specimen and users, and collecting the samples on the 28.8-Kbaud of remote modem connection. They also identify the authentication problems via keystroke faced by

the user. They presented the dynamics technique of new keystroke analysis methods which help to solve various the problems associated with keystroke analysis: The chances of typing errors and the typing intrinsic are variability. An authentication system using the help of this scheme described in this article does not require any particular tuning, nor a learning training to work with a specific set of genuine users of the system. This tuning is possible, by increasing the strength of the system to authenticate genuine users and reject fraud. The text used in theirs experiments is too long which can be used for replacing the password based authentication system, meanwhile its length is admissible for other applications.

• H.-M. Sun, An efficient remote use authentication scheme using smart cards, IEEE Trans. Consumer Electron.46 (4) (2000) 958–961.[27]

They Proposed scheme which is fully based on the discrete logarithm mechanism, Hwaiig and Li [28] suggested authentication for remote user using smart cards. In this paper, the author suggested a more efficient and more practical authentication scheme by using smart cards. The proposed scheme significantly minimized the communication and computation costs. Moreover, the password length in scheme is 64 bits which is very easy to memorize by the user. They also suggested the problems lies in Hwaiig and li scheme [28].Once the problems of discrete logarithms is solved, Hwaiig and li scheme can be destroyed.

• J.K. Jan, Y.Y. Chen, 'Paramita wisdom' password authentication scheme without Verification tables, J. Syst.Softw. 42 (1998) 45–57.[33]

They present the most efficient practical methods to unlock the problems related to the authentication with the help of public key and public key distribution. Users can able to change theirs password freely. The password length suggested in the scheme should be appropriate for memorization and the methods can be easily adopted in with change in the technology easily. The user doesn't share theirs private key over networks. The scheme is totally based on the public key. The main problems lies in the scheme is with the password should of fixed length and once the user's credentials gets compromised the system can be destroyed. Buddha words of wisdom are the main concept used in this scheme in order to avoid compromisation of the credentials.

3.1 SECURITY

In general, security means the conditions of being protected against any loss or danger. It is basically similar to safety. The word security is synonymous with safety. Technically security means that something's which is not only secure but also has been secured. Security defines as "the quality or sate of being secure to be free from any danger". As far as internet security is concerned there are various area where it can be addressed like computer security, data security, application security, information security and network security etc. Each and every successful company should have the following level of security and they are pointed below [1, 11, 17, 19, and 24]:

1. Physical security which addressed the physical items objects, and the area of company from unauthorized access or misuse.
2. Personal security involves in the protection of the users, clients and individual or group of individuals who are unauthorized to access the company and its operations.
3. Operation security deals with the protection of operation of the details of particular process or series of activities
4. Communications security deals with the protection of the company's media, technology, contents etc.
5. Networks security and information security are one the major security that needed to be covered in this papers and are explained clearly.

Security experts helps to protect their environment as efficient as possible. They primarily focus on protecting confidentiality, integrity, and availability (CIA) or say maintaining CIA.

- Confidentiality assure that no data has been exposed to other either intentionally or unintentionally.
- Integrity assure that no changes made in the data by any unauthorized person. Data remains the consistent in both internally and externally.

- Availability assure the availability of the data and must restrict access to the unauthorized person.

Moreover, the virus is one the basic threats to the security system. : " *A virus may be introduced into the system physically when it arrives on a diskette or optical disk and is subsequently loaded on to a computer. Viruses may also arrive over an internet .In either case once the virus is resident into a system, internal security tool are needed to detect and recover the system".*

3.1.1 What is Information Security?

Information is the life blood of the modern world. Each and every person even organization possess critical or sensitive information. The word Information security described as "*The task of protecting and securing the digital information which is typically generated by the computer system like personal computer , smart phones , stored on the physical device like hard disk optical disk, flash disk and further can be transmitted over the network either on secure or unsecure channel.*"

It act as protective layer for our digital data and protect of information .information must be protected because it has value. There are there characteristics of the information which needed to be protected accordingly.

- Confidentiality assure that no data has been exposed to other either intentionally or unintentionally.
- Integrity assure that no changes made in the data by any unauthorized person. Data remains the consistent in both internally and externally.
- Availability assure the availability of the data and must restrict access to the unauthorized person.

3.1.2 What is Network Security?

Network security refers as the protection of the data, information, networking components, connections and contents. We can also state a network security is the security of the information of the networks system hardware, software, and system data from being accidentals or malicious destruction [4]. The content of the network security also deals with

both technical aspect of the problems and the management issues. Network security also deals with the different issues depending up on the different environment and they are pointed below:

- Operating system Security.
- Network information Security.
- Information dissemination on the Network Security.
- Network security of the content of the information

3.2 PROBLEMS STATEMENTS

If user leaves the system without logging out or locking the system session, an intruders can get a golden opportunities to use the system and get access to the resource without any problems. Now a days 2 level verification technique is very much common. Have you ever lost your smart phone or cell phone? The 2nd layer verification protocol deals with the addition of securities features added to the smartphone or cellular phone since the code generated by the system for 2nd layer verification is send to the mobile device and valid for once use within a fix time stamp. In traditional password system, every user was assigned with a user id and a passwords. If he/she want to s login he/she has to submit id and passwords. Remote server compare the identifier of user and the data of the respective table in the database if found correct, it authenticate the user and provide control to users and allocate the resource to them. The users' identifiers are stored in the forms of plain text in the table of the database. To prevent the stealing of the data hashing is done on the table .further is found that hashing is also not very much secure. To overcome on the types of problems the concept of 2 level authentication system is developed and that's called One Time Password [8, 15, 17]. The main problems that we found while reading the papers are that, none of the technique is safe to make secure the authentication .Either some can be broken by brute force attack or some can be broken by dictionary attack .Latest research Papers published on for the authentication are fully based on Password hardening [2, 25, 30, 35, 37] or time legacy of the password. From that algorithm special types of pattern are gets generated and authentication works on the basic on that. If the text and pattern matched then only we can able to access the resources [19]. Generally talking there are 3 types of identity authentication methods and they are: Identity authentication of something

known, Identity Authentication something's possess and last one deals with the personal characteristics. On combining above criteria we can able to enhance the security level.

3.3 METHODOLOGY

Following are the methodology which has been followed are consist of the following and further explained in details in coming chapters:

1. A literature review.
2. Research Approach
3. Data collection.
4. Data analysis
5. Testing.
6. Result and Analysis
7. Conclusion and discussion

We have developed two scheme to solve the issues currently being faced by the users and fear of loss of integrity confidentialities. Till date each and every scheme had probably deals with the securing the data and credentials during the transmission phase like encryption, decryption, hashing etc. but none of the scheme deals with the protection of passwords and One time Passwords even if compromised .End to end protection system has not been developed till date .We have worked to protect the users data's, authentication, authorization of resources even if the passwords is compromised. Our main aim to develop such algorithms which can protect the system even if password is hacked or compromised .Let's say our ids is "ABC" and password is "XYZ". Whenever anybody come to know id and Password by any mean he or she can easily logged into the system. This is universal system of authentication. But system is deals with the protection even if the passwords known by intruders. Using the same identifiers the genuine user can log into the system but with the same identifiers the intruder's failed to log in to the system. This is the first basic concept of out scheme. Now second phase deals with the OTP protections. We found that OTP is not secure at client side. Whenever we initiate the transections of bank or reset our ids we receive the **SMS** containing 4-5digit code that is valid for a fix session and for one time .In case if that cosde is compromised the intruders easily can get access. We worked hard and come to a great solution to secure both of them. We added a time element

inside the password to protect even if the password is compromised .It is very much efficient since none of the known attack till date can crack it because time element that we added in the scheme can't be traced either in database or during transmission or by phishing the passwords. As far as OTP is concerned we have also develop a technique to protect the OTP or reset code at client side even if the OTP is compromised. For the protection of OTP we added Random logic Table whose gets changed at each iteration.

3.4 SCOPE OF THE STUDY

The Study of the research is basically deals with the modification of **O**ne **T**ime **P**assword and time elements inside the password. In Previous OTP technique, there are a lots of **Vulnerabilities in the Text based password scheme and OPT**. If the OTP is accessed by anybody, he/she can easily access the account. The study helps in me developing the new pattern which helps in the securing the OTP. OTP is used for resetting the account passwords, Authenticating the Transections and many more. OTP or Reset code is send to the user Mobile or Email ids and further the action is taken. But what if you're mobile is stolen by some body or mistakenly email id is hacked? The intruders can easily Reset the passwords or authenticate the transection easily. This is the main vulnerabilities of the OTP or Reset Code. Though they are not easily crack to Reply Attack. This proves that an intruder who maintain control over an OTP which was used to log into a service or to do a transaction will not be able to abuse it, since it will no longer be valid. OTPs are very hard to memorize for human beings. So it requires some more additional technology to work. The generation of OTP algorithms basically makes the uses of pseudo randomness or randomness, making prediction of successor OTPs by an attacker difficult, and it also use hash functions, which is further can be used to generate or derive a value and are hard to reverse back in the original mode. Therefore difficult for an intruders to get the data that was used during Hashing.

3.5 OBJECTIVE THE STUDY

With the raise of information level continuously, the importance of information and network security growing at high ratio and has reached to the peak point. It has now become the national security. They have affected the human's works, life and even affect the

country. Even though, the security regarding the information has not been optimized till now. It has been serious issue to safeguard our information and system and networks. Effectively protection of critical information and data and safe the system are the major task and it should be considered seriously .after reading the survey and published research papers on OTP and text based passwords authentication scheme, we found none of the technique is fully secure. Each and every Algorithms deals with the technique for the formation of the OTP till now and securing the password during the transition and at server side, but none of the Technique tries to secure the OTP from being hacked and passwords being compromised. Though the Hashing function are used to rid of it but the main problems is with the code that are send to the email or on the mobile via **sms** or by phone call or any mean. Even after Database is accessed by the hacker/Attackers they won't able to detect the Reset code or OTP since they are in Hash. But the main problems arise at the End User side not at the server side so the main works of the study is done to solve the problems that are occurs at the users side and protect them we mean client side .The chief the judicial of the research is to find the problems which are still on ongoing algorithms and to develop more secure algorithms for the protection of the data and system. During reviewing the literature I have found many problems related to the technique which is unsolved and asked by the researcher to work on it. The proposed algorithms which is developed taking help from the previous technique and is comparatively more secure and hard to crack. The Algorithms deals with the End user side. Attacker can easily divert the users to get the OTP / Reset code form them and further they can do whatever they wish.

3.6 APPLICATIONS

Researches are basically done in order to solve the issues related to the previous problems to find the weakness in already developed scheme and further to make them efficient. Followings are the applications and advantages of our new developed scheme.

1) Cryptanalysis is about to **impossible**. Time elements that we added can't be traced by any attack. Without the addition of that element during authentications user cannot log into the system. Even if Passwords transmitted over channel in the form of plain text or in the forms of cipher text. The time element is (α, β, θ) remains safe to the user which is back bone of the scheme. Now talking about the second phase, it deals with

the secrete keys; one is generated by the system and another can be freely chosen by the user and it will acts as the decryption key for the OTP.

2) It can be used in very complex system where high security matters. Authentication are applied in all classes because it is the act of identifying identity. Our scheme can be use from low level to high level organization depending upon the needs. It is bit complex and hard to memorize by the individuals so low level organization can use our first scheme and high level can use both scheme. We can use this scheme in area such as nuclear plants, Defense, Banking, Emails System, etc.

3) There should be two mode in which if the time elements as well password matched , interface will be can be accessed in both mode that's Read and Write mode .If just password is matched the interface can be accessed only in Read mode and some features kept hidden else authentication Failed.

3.7 LIMITATIONS

1) Transmission delay may create problems during authentication.
2) Use of Time element within the passwords may be increase the complexity of the scheme.
3) User has to remember a lots of no of identifiers like id, password, time element, user key, system generated key etc.
4) In this paper we have covered the security and usability measurement in real time scenario.it doesn't work on non-real time environment.

CHAPTER 4: PROPOSED ALGORITHM

There are many schemes proposed and developed to authenticate a genuine user, but none of them seems to be efficient and reliable and flexible. Similarly Chang and Wu developed a scheme which is called remote password authentication scheme using Chinese Remainder Theorem (CRT). It does not store verification password table and protect against reply attack. In this scheme user cant chose their passwords and change them freely. The main problems with the scheme is that it failed if the passwords are compromised.

4.1 DESCRIPTIONS

In this Paper, we first cover the following 10 requirements for evaluating the new password authentication scheme. These 10 requirements tries to solve all the problems of text-based passwords scheme and OTP based password scheme [13]. Each of them are equally important and independent.

A1 : The password or verification database table are not stored in the server.

A2 : The Passwords can be chosen and freely updated by the user.

A3 : The password cannot be fetched by the admin of the server.

A4 : The passwords are not transmitted in plain text on network.

A5 : No one can impersonate a legal user to login the server.

A6 : The scheme must resist the replay attack, guessing attack, modification attack, and stolen- verifier attack.

A7 : The length of a password must be appropriate for memorization.

A8 : The scheme must be efficient and practical.

A9 : Intruders can access the system even if password is compromised.

A10 : Intruders can access the system even if OTP is compromised.

In addition, our new scheme has been intended to be more efficient to the previous scheme in terms of time, storage, utilization, computations complexity. We have proposed 2 algorithms in this paper and they are pointed below

1. 4D Password Security Algorithms.
2. OTP securing at end user side/ client side.

4.1.1 ONE WAY HASH FUNCTION [13, 34, 6]

A one way hash function state that h1: x->y is a function with the following properties.

- The function h1 takes the message of limited length as the input from the user and further produces the message digest of fixed- length size as output.
- The function h1 is the one way hash function and further computation output h1(x) =y.
- Computationally x is infeasible to find x' such that x' not equal to x but h1 (x') =h(x).
- To find the any pair of x.x' such that such that x' not equal to x but h1 (x') =h(x).

4.1.2 Time Element - 4D

There are 3 spatial dimension; x-coordinates, y-coordinates and z- coordinates. They can be labeled with the any forms chosen form length, height, depth, width. It also used in positing the element in a plane mirror. Later on it is found that one more dimension exist in the universe that called time dimension or space time. We have used the concept of space time in our scheme to make it more efficient and reliable. Since time is measured but can't be seen it helps us in our project very efficiently for making it more better the previous proposed scheme.

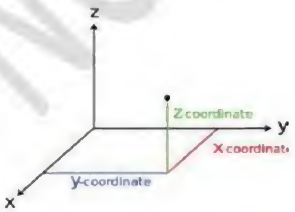


Fig 4.1: 3D Plane

We have consider the time element for the scheme that are represented by the geek Latin word. Like α, β, θ and so on. This elements store the time (sec) inside the passwords which prevents from every types of known attack discovered till now.

4.2 4D-AUTHENTICATION SCHEME

Our scheme consist of basically 3 phase.

- Registration phase.
- Authentication phase.
- Password change phase.

4.2.1 Registration Phase

This phase deals with the registration or admission of the user to the server with required credentials. Once the registration phase completed user is assigned theirs details so that further user can authenticate himself to the server within a given time periods.

4.2.2 Authentication Phase

This is one the important phase in which users can get the access control or resource allocation from the server. During this phase users need to input theirs credentials like user id passwords along with the time elements and send request to the server [13, 12]. The remote server compare the inputs with the stored one form tis database and reply with true to the user. After successfully clearing the first phase user need to request to generate the one time password from the server. Server further takes the request and generate the one time password and encrypt with secrete keys which is generated from the user_id id and passwords of the user and send back to user. User need to decrypt the one time passwords and need to send back again the decrypted key to server. Remote server again compare with the database and return true if matched.

4.2.3 Password change Phase

This phase equally important. It deals with the changes made in the users stored credentials like passwords. Users are free to change and modify their credentials. No any extra efforts are required for this phase. Whenever user changes theirs credentials the secretes keys automatically gets changed and further we can conclude that even if the system is compromised user can changes theirs credentials with in no time and secure their account.

So let's first discuss about 4D password authentication scheme. It is have been explained briefly describe the basic steps and concepts of 4D authentication in the following points:

1. User select the user ids and passwords as per theirs requirements.
2. System ask to insert the timer between the each character of the passwords. (Let range from 0-15sec). So that while entering the password, he/she has to input the keys of passwords after specific time.
3. System runs the one-way hash function and hash the identifiers (user id, passwords).

4.3 ONE TIME PASSWORD

A one-time password (OTP) is a kind password which is works for only one session or transaction, on system or other electronic digital device [9]. OTPs may be in the forms of number or character that are associated with traditional (static) password-based authentication. It is implemented for providing the two factor authentication security to the user. The most significant advantages of the one-time password is they are not vulnerable to reply attack. It is valid for only one session. The main aim of one time password is to secure user account if credentials are compromised or hacked by the user [1]. One time passwords easily can't be intercepted by any hacker unless and until the device receiving the OPT is not stolen or theft. It danger if device is stolen or email is hacked. It has enhanced the traditional authentication password system.

4.3.1 OTP Generation

OTP generation algorithms uses pseudo randomness or randomness function which is associated with the user's data. It is easy to predict the OTP by looking previous one so randomness function is used to prevent it. Some of the OTP generation algorithms are as pointed below:

- HMAC-based One-time Password Algorithm
- Time-based One-time Password Algorithm

We have considered HMAC–based Onetime password Algorithms for our scheme since Time- Based One-time password algorithms are vulnerable. They can be captured using

the malware if installed on the devices. It can also be read by any person without unlocking the devices.

4.3.2 HMAC-Algorithms overview [34]

This section explain an algorithm which is used to develop Time-synchronized OTP values which is based on SHA-1 hash function and Hash Message Authentication Code (HMAC). This is also called HMAC-Based One-Time Password. OTP is generated is fully based on HMAC. One-Time Password is no doubt one of the easiest and most popular methods of 2-factor authentication that is used for securing access to accounts from hacker or unauthorized users. One-Time Passwords are often referred to as one of the secure and stronger technique of authentication, and can be easily installed across multiple machines including home computers, mobile phones etc. When the user login to the system, OTP is generated and sent back to the user's e-mail id or mobile phone in the forms of sms. The user is then directed to next step to enter the OTP. If the OTP is verified, the user get access to system and its resources.

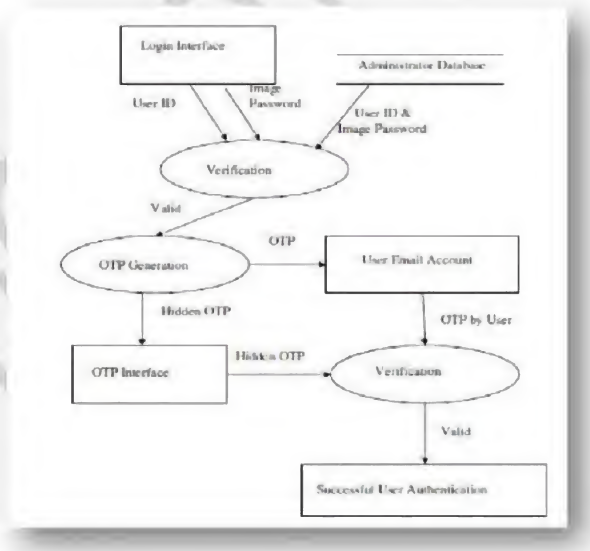


Fig 4.2: Data flow diagram

Algorithm Requirements

X1 - The algorithm MUST be time synchronized.

X2 - The algorithm SHOULD be economical and easy to implement.

X3 - The algorithm MUST work efficiently.

X4 - The value displayed email or sms should be easy to read and entered by the user. For this the OTP value should be of flexible length such as a 4-digit or 6 digit value

X5 - User-friendly environment.

4.4 ALGORITHMS OF 4D AUTHENTICATION SCHEME AND HMAC-OTP

Let consider the user Id and Password are ABC, XYZ respectively. α, β, θ are the time storing element (in sec) and are inserted between the XYZ, i.e. αXβYθZ.μ (sec) is the total time required to input the password.

Whenever user input the password XYZ to the system, thought it seems to be right but system cannot validate the user because he/she has to wait for α, β, θ sec before pressing the each key of the password and also total no of digit of password with in the μ (sec) time .In order to get control on system or Resources, the user has to input the key password after α, β, θ sec.The proposed Algorithms contains the following basic steps:

1. Registration Phase.
2. Login or Authentication Phase (Using UId, Pwd, OTP)
3. Services Request.

Notation: The following notation are used though out the paper.

Table 4.1: Notations and summary

Notation	Description
U	User/client
UIDc	User Identifiers
PWD	User Passwords

α, β, θ……	Use to store the time element between the keys of passwords
μ	Total time to input the password in the system.
H	Hash functions.
RMS(1……x)	Remote Servers, Services Servers.
Ukx	User Secrete Key.
Kx(1….x)	Computer Generated Key.
i,j	Rows and columns value.
OTP	One time Password.
FN	Any Function.
T	Time Factors
OTPx OTPy	Encrypted OTP Decrypted OTP
TOK	Token
OHMK	OTP generation Algorithm
U	User/client

Here, we have developed algorithms for authentication schema based on 4D (time dimension), OTP and random table. Proposed works are listed below. The proposed Algorithms that contains the following basic steps:

1. Registration Phase.
2. Login or Authentication Phase (Using UId, Pwd, OTP)
3. Services Request.

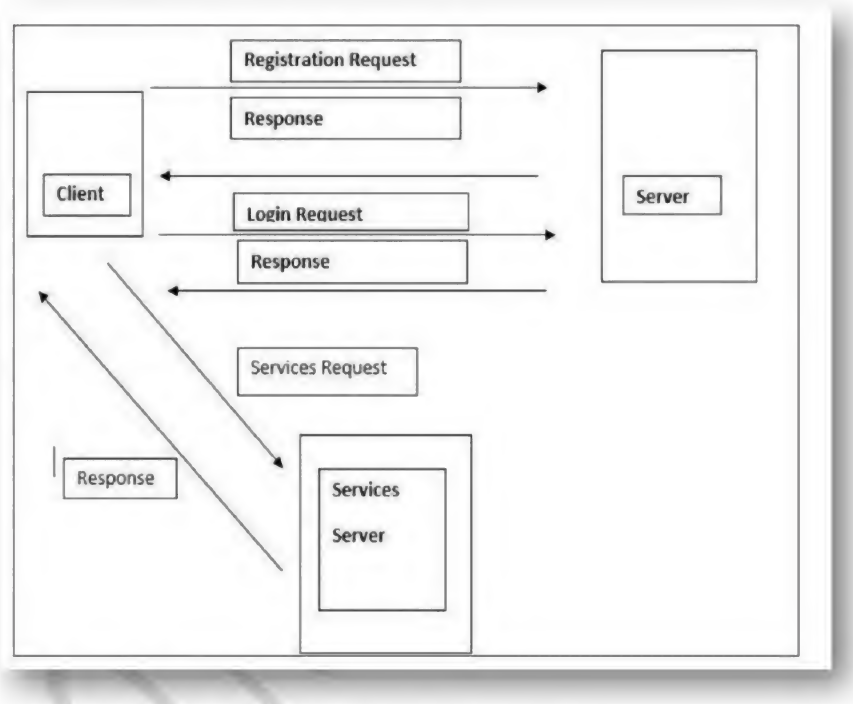


Fig 4.3: Authentication flow diagram

4.4.1 Registration Phase

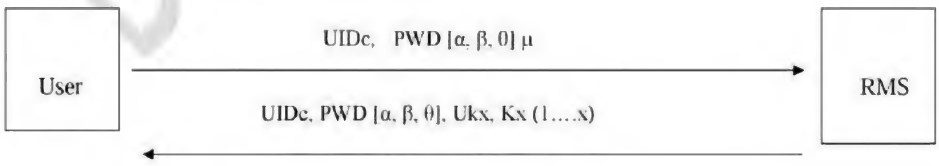


Fig 4.4: Registration Phase

STEP 1:

- User /client choose UIDc, PWDc, [α, β, θ] μ, User secrete key (Ukx) and sends them to a Remote server (RMS1) over a secure/unsecure channel.
- RMS1 Store the identifiers UIDc and PWD along with [α, β, θ] μ where PWD= h (PWD) (h=hash).

STEP 2:

- RMS1 Server Generate Secrete Key K1; K1= FN {UIDc, PWD}; 1 digit.

STEP 3:

- Store UIDc, h (PWD) [α, β, θ] μ, K1, Ukx (i, j) -> Database.

STEP 4:

- Ukx: User Secrete Key; 1 Digit.
- Send Back the Information to the user i.e. (UIDc, PWD, [α, β, θ] μ, Ukx, Kx (1....x))

Note: Further K1, and Ukx will act as the Value of the Random table's rows and column (i, j);
Where i=K1 and j=Ukx.

4.4.2 Authentication Phase

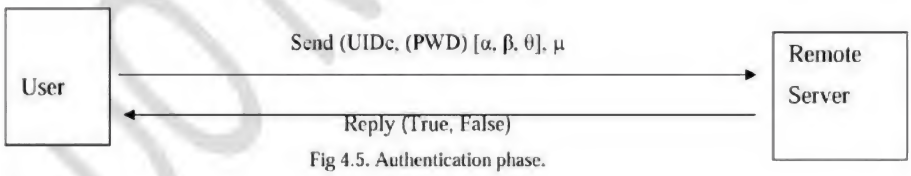


Fig 4.5. Authentication phase.

- Reply = True.

Then,

-Request (OTP) ⟶ RMS Generate OTP and encrypt it to OTPx (i, j).

-User [OTP] ⟵ Send [OTP] Back to User.

-User Decrypt

OTP to OTPy ⟶ Send OTPy to RMS.

If OTPy==OTPx, Return True.

-Login Success

STEP 1:

- Input UIDc, PWDc [α, β, θ] with in μ time.
- Submit to Remote Server.
- If UIDc, PWD [α, β, θ] μ Found Correct, Server Reply (True), If Incorrect, Failed.
- User request to generate the OTP from Remote Server (RMS).
- Server Generate OTP Using HMAC Algorithm and Encrypt OTP with the value fetch from random table [i, j] and hash it and store in forms of OTPx in Database.
- Server Send OPT back to the User.
- User Decrypt OTP using the same Random table with (K1, Ukx) value and form OTPy
- User Send OTPy to the RMS.
- RMS server compare OTPy with OTPx.

If Found Correct.

- Reply Success, Generate a Token (TOK) valid for Time (T) and Authorized Services to the user.

- Else Failed to Authenticate

4.4.3 OTP Generation Phase

Following are notations used in the OTP generation algorithms

Table 4.2:.HMAC Notations

Symbol	Description
T	Represent the time
Key	Secrete key shared between client and server.
Digit	Output digit value

4.4.3.1 Description [34]

This algorithm is fully based on increment on time value function and a static symmetric key known only to client and server. To generate OTP value, a HMAC- SHA-1 algorithm is used. The result of the HMAC-SHA-1 is 160 bits, so we have to truncate the value get the smaller digit.

OTP (Key, T) = Truncate (ToHex (HMAC-SHA-1(Key, T)))

Where –Truncate function converts the value generated through HMAC-SHA-1 to an OTP value.

4.4.3.2 Generation of OTP Value

The algorithm can be explained in 3 steps:

Step 1: Generate the HMAC-SHA-1 value Let HMK1 = HMAC-SHA-1(Key, T) //
HMK1 is a 20- byte string.

Step 2: Generate a hex code of the HMK.
HexHMK1=ToHex (HMK1).

Step 3: Extract the 8-digit or 6-digit OTP value from the string.

OTP = Truncate (HexHMK1).

Step 4:
-Store OTP ->Database
-Encrypts OTP with (K1,Ukx->i,j); OTPx={OTP,(i(k1),j(Ukx)].
-Send OTP to the User not **OTPx**

4.4.3.3 Operation

MessageDigest md1 = MessageDigest ("SHA1")
md1.update (Key, T).
Output = md1.digest().
buf_1 = hexDigit((output >> 4) & 0x0f).
Otp=buf_1.toString ().
Otp=otp.substring (0, 7).

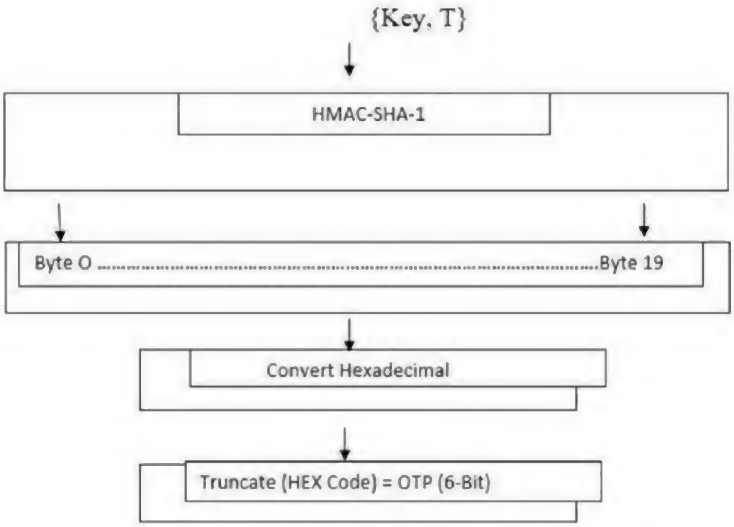


Fig 4.6. OTP Mechanism

Note: Further K1, Ukx will be the Value of Rows and Column of Random Table Generated during the Authentication

4.4.4 Password Change Phase

Step 1:

- Login to the System.
- Initiate Password Change Interface.
- Enter Previous (PWD) [α, β, θ] with in μ time.
- Encrypted OTP is generated.
- Decrypt OPT
- On Valid Decryption; change the (PWD) [α, β, θ] μ with new one
- Generate New K1; Overwrite old K1.
- Ukx Remains Same. Send back to the user.

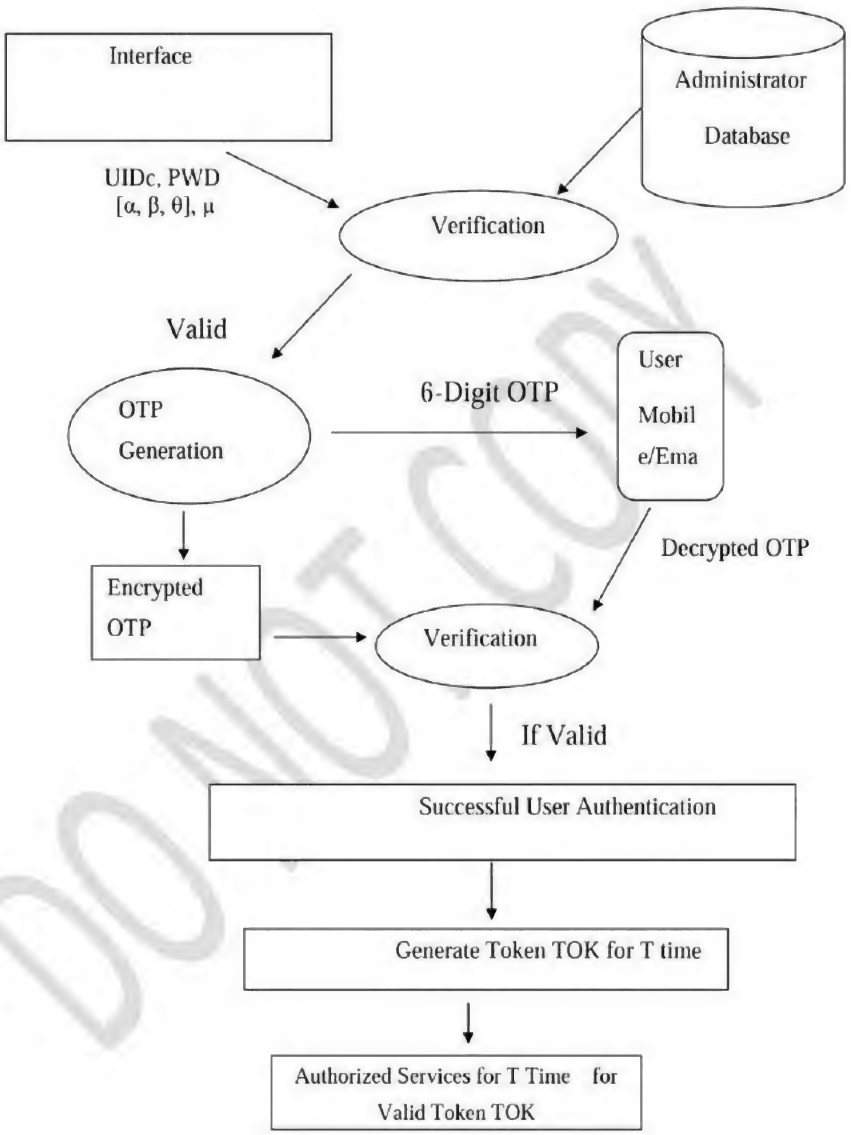


Fig 4.7: Algorithms summary

5.1 CRYPTANALYSIS

Cryptanalysis is the study of examine information systems in order to study the mystic aspects of the systems. Cryptanalysis is used to break cryptographic security systems and gain control system and its information, even if the key is not known. In mathematical study of the algorithms, it includes the study of channel attacks that do not target weaknesses in the cryptographic algorithms themselves, but instead exposed the weaknesses in their implementation. Cryptanalysis refers to the study of ciphers, cipher text, or cryptosystems (that is, to secret code systems) with a view to finding weaknesses in them that will permit retrieval of the plaintext from the cipher text, without necessarily knowing the key or the algorithm [31].

5.1.1 Role of Cryptanalyst

A discipline related to cryptography is cryptanalysis, defined as the methods of extracting cipher text. These two streams combined to form the science of cryptology. The cryptographer's deals with security for information by making strong cryptosystems, while the cryptanalyst's deals with the weaknesses or flaws in the developed cryptosystems and breach the security implemented on that system. Professional cryptanalysts work is to perform an important character in evaluating and conforming the strength of cryptosystems. In fact, cryptosystems are generally not considered to be more secure until and unless they confront remarkable cryptanalysis. Cryptanalysts can use the most powerful computing system and a different types of procedures, processes, and techniques to start attacks on the system. In fact, a skilled cryptanalyst can even decide plaintext from samples of cipher text without even getting the cipher which was used to generate it. Cryptanalysis can also be used illegitimately for unlawful gain. Highly trained intruders can use cryptanalysis methods as part of their attacks security systems. When properly deployed, standard cryptography-based security methods can provide sufficient protection against a wide range of attacks, inclusive common cryptanalysis methods. However, to get highly valuable data, highly trained intruders or trained intelligence agents with use of

powerful computing system might have the motive to start expensive and highly advanced cryptanalyst attacks. Stopping such advance cryptanalyst attacks requires extremely secure systems which use powerful cryptography-based security technologies.

5.2 OBJECTIVE OF MODERN CRYPTOGRAPHY

None of computing system of cryptography, called a cryptosystem, can be believed to absolutely unbreakable or above compromise. However uncertain a successful attack might seem, there are always some surface of the cryptosystem that can be compromised. The history of cryptography is full of examples of security that were once included in the group of powerful technique, and yet intruders were able to creak the security of the system and compromise theirs credentials [20]. Since the cryptographers are not fully aware of all kind of attack, they cannot develop and deployed cryptosystems in real life that are assured to have no weaknesses or that are impermeable to unforeseeable technique of attack. Furthermore, crypto security systems must be successfully deployed the real word, so they can be subject to real-world limitations, restrictions and constraints. Each and every security systems, including cryptography-based security, have weak point that can be hacked and potentially exposed and exploited.

The main aim and goal of modern cryptosystems is not to supply complete and perfect or risk-free security. Rather, the objective of cryptography-based security is to secure and protect information and the resources by restricting the unauthorized acquisition of the information system or tampering with the information which are more costly than the potential value that might be obtained. Since the worth of information usually decreases over time, better cryptography-based security preserve information until its value is potentially less than the cost of illegal seek to get or tamper with the data and information. Good cryptography, when perfectly deployed and used, it may secure our information and system up to some extent. For example, many latest cryptosystems make it very hard but not impossible for an intruders to obtain the keys or passwords. Although the key might be eventually decided by a highly skilled person, given more time and effort, cryptosystems can still provide high security to protect our worthy information and systems. Intruders can feasibly guess the correct decoding key or password, the cost for the intruders would be much more than the value of the information which is being secured by the key or

password. For well- evaluated, well-designed, and analyzed cryptosystems without any unknown weakness, the primary protection against any attack is dependent on length of the passwords or the secrete key. Cryptosystems having the secrete keys shorter than the plaintext are subject to comprehensive search attacks where the intruders tries all possible combinations of the secrete key until it found. For large password or secrete keys, a strong search for the key basically requires smart and expensive computing device to conduct brute force attack , and the attack can take up to thousands or even millions of years to complete. Cryptosystems can protected against brute force attacks by simply increasing the length of the password or secrete key which is enough to make the implementation of the attack computationally infeasible or cost-prohibitive. Another objective of all security systems, including cryptography-based security systems, is to secured and protect information and the resources at less cost than the value of the information which being protected against any attack. A cryptography-based security system must feasible and efficient which can provide security at acceptable costs.

5.3 SECURITY FUNCTIONS OF CRYPTOGRAPHY [11]

Cryptography is most frequently related with the confidentiality of information and data which it provides. However, cryptography provides the following four basic functions:

5.3.1 Confidentiality

It helps to assurance that only approved person can read or use confidential information. Without confidentiality, anyone with proper network access can use tools to eavesdrop on network and capture the valuable information. Intruders who gain illegal network access and permissions can steal the information which is stored as plaintext or transmitted over channel. In order to prevent, Systems use methods and mechanisms to protect the information confidentiality. So the technique of encryption is used to prevent confidentiality.

5.3.2 Authentication

It is necessary to verify the identity of the entities which exchange the data over the network. Without authentication mechanism, anyone having network access can use

required available tools to forge Internet Protocol (IP) addresses and mimics others. Therefore, Systems use various methods and mechanisms to authenticate both the user and server who receive the information.

5.3.3 Integrity

It verify that the original structure of information have not been corrupted, tempered or altered. Without integrity, anyone may change the information or information become corrupted, and further the alteration could remain undetected. So in order to prevent many Systems use methods and mechanisms to verify the integrity of information. Digital signature is one of the best for it.

5.3.4 Nonrepudiation

It assurance that a party during communication cannot deny that a part of the actual communication happened. Without nonrepudiation, anyone can communicate and then later either may deny the communications fully or claim that it might have happened at a different time. To provide facilities, systems must produce the evidence of proof of communications and transactions that happened, so that involved person cannot easily refuse it[24].

5.4 BRUTE FORCE ATTACK ON PREVIOUS SCHEME [6]

How long will your password stand up? This the main question which can arise in our minds. As we have proposed two algorithms so we need to first discuss about the possible attack on the 4d scheme. Before moving forward we need to have a look out the passwords recovery speeds. Below following tables describe about it.

Classes of Password per Sec Brute force Attack

Class A. 10,000 Passwords/sec

Typical for recovery of Microsoft Office passwords on a Pentium 100

Class B. 100,000 Passwords/sec

Typical for recovery of Windows Password Cache (.PWL Files) passwords on a Pentium 100

Class C. 1,000,000 Passwords/sec

Typical for recovery of ZIP or ARJ passwords on a Pentium 100

Class D. 10,000,000 Passwords/sec

Fast PC, Dual Processor PC.

Class E. 100,000,000 Passwords/sec

Workstation, or multiple PC's working together.

Class F. 1,000,000,000 Passwords/sec.

5.4.1 Brute - Force 10 Character Length

Numerals	0 1 2 3 4 5 6 7 8 9

Table 5.1.: Brute force 10 Character numeric password brute force.

	Password	Class of Attack					
Length	Combinations	Class A	Class B	Class C	Class D	Class E	Class F
2	100	Instant	Instant	Instant	Instant	Instant	Instant
3	1000	Instant	Instant	Instant	Instant	Instant	Instant
4	10,000	10 sec	Instant	Instant	Instant	Instant	Instant
5	1 Million	$1^{1/2}$ minutes	10 sec	Instant	Instant	Instant	Instant
6	10 Million	17 minutes	$1^{1/2}$ minutes	$1^{1/2}$ minutes	Instant	Instant	Instant
7	100 Million	2 ¾ hours	17 minutes	$1^{1/2}$ minutes	10 sec	Instant	Instant
8	1000 Million	28 hours	2 ¾ hours	17 minutes	$1^{1/2}$ minutes	10 sec	Instant

5.4.2 Brute - Force 26 Character Length. Either upper or lowercase.

Upper Case Alpha	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Lower Case Alpha	Abcdefghijklmnopqrstuvwxyz

Table 5.2: Brute Force 26 Character Length Brute force

	Password	Class of Attack					
Length	Combinations	Class A	Class B	Class C	Class D	Class E	Class F
2	676	Instant	Instant	Instant	Instant	Instant	Instant
3	17,576	< 2 Sec	Instant	Instant	Instant	Instant	Instant
4	456,976	46 Sec	5 Sec	Instant	Instant	Instant	Instant
5	11.8 Million	20 Min	2 Min	12 Sec	Instant	Instant	Instant
6	308.9 Million	8½ Hours	51½ Min	5 Min	30 Sec	3 sec	Instant
7	8 Billion	9 Days	22 Hours	2¼ Hours	13 Min	1 ¼ min	8 sec
8	200 Billion	242 Days	24 Days	2½ Days	348 Min	35 Min	3 ½ Min
9	5.4 Trillion	17 Years	21 Months	63 Days	6 ¼ days	15 Hours	1 ½ Hours

10	141 Trillion	447 Years	45 Years	4½ Years	163 days	16 days	39 ¼ Hours
12	95 Quadrillion	302,603 Years	30,260 Years	3,026 Years	302 Years	30 Years	3 Years
15	1.6 Sextillion	53 Trillion Years	532 Million years	53 Million Years	5 Million Years	531855 Years	53185 Years
20	19.9 Octillion	63 Quadrillion Years	6.3Quadrillin Years	631Quadrillion Years	631 Trillion Years	6.3 Trillion Years	631 Billion Years

5.4.3 Brute –Force 36 Character length. Either upper or lower pulse numbers

Table 5.3: Brute Force on 36 character length

	Password	Class of Attack					
Length	Combinations	Class A	Class B	Class C	Class D	Class E	Class F
2	1296	Instant	Instant	Instant	Instant	Instant	Instant

3	46,656	4 Sec	Instant	Instant	Instant	Instant	Instant
4	1.6 Million	2 ½ min	16 sec	1 ½ sec	Instant	Instant	Instant
5	60.4 Million	1 ½ Hours	10 min	1 min	Instant	Instant	Instant

5.4.4 Brute –Force 52 Character length

Mixed Alpha	AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYxZz

Table 5.4: Brute Force on 52 character length.

	Password	Class of	Attack				
Length	Combinations	Class A	Class B	Class C	Class D	Class E	Class F
2	Instant	Instant	Instant	Instant	Instant	Instant	Instant
3	140,608	14 Sec	< 2 Sec	Instant	Instant	Instant	Instant
4	7.3 Million	12½ Min	1¼ Min	8 Sec	Instant	Instant	Instant

5	380 Million	10½ Hours	1 Hour	6 Minutes	38 Sec	4 Sec	Instant
6	19 Billion	23 Days	2¼ Days	5½ Hours	33 Min	3¼ Min	19 Sec
7	1 Trillion	3¼ Years	119 Days	12 Days	28½ Hours	3 Hours	17 Min
8	53 Trillion	169½ Years	17 Years	1½ Years	62 Days	6 Days	15 Hours
9	2.7 Quadrillion	8,815 Years	881 Years	88 Years	9 Years	322 Days	32 Days

5.4.5 Brute –Force 62 Character length. Mixed upper, lower and numbers

Mixed Alpha	0123456789AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYxZz

Table 5.5: Brute Force on 62 character length.

	Password	Class of	Attack				
Length	Combinations	Class A	Class B	Class C	Class D	Class E	Class F
2	3,844	Instant	Instant	Instant	Instant	Instant	Instant
3	238,328	23 Sec	< 3 Sec	Instant	Instant	Instant	Instant

4	15 Million	24½ Min	2½ Min	15 Sec	< 2 Sec	Instant	Instant
5	916 Million	1 Day	2½ Hours	15¼ Min	1½ Min	9 Sec	Instant
6	57 Billion	66 Days	6½ Days	16 Hours	1½ Hours	9½ Min	56 Sec
7	3.5 Trillion	11 Years	1 Year	41 Days	4 Days	10 Hours	58 Min
8	218 Trillion	692 Years	69¼ Years	7 Years	253 Days	25¼ Days	60½ Hours

5.4.6 Brute –Force 86 Character length. Mixed upper, lower and numbers

Mixed Alpha and Symbol	AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYxZz< SP>!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~

Table 5.6 Brute –Force 86 Character length

	Password Combinations	Class of Attack					
Length		Class A	Class B	Class C	Class D	Class E	Class F
2	7,396	Instant	Instant	Instant	Instant	Instant	Instant
8	2.9 Quadrillion	9,488 Years	948 Years	94 Years	57 Years	346 Days	34 Days

5.4.7 Brute –Force 94 Character length. Mixed upper, lower, numbers and symbol

Mixed Alpha Number and Symbol	AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwX xYxZz<SP>!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~0123456789

Table 5.7 Brute –Force 94 Character length

	Password	Class of	Attack				
Length	Combinations	Class A	Class B	Class C	Class D	Class E	Class F
2	9,216	Instant	Instant	Instant	Instant	Instant	Instant
3	884,736	88½ Sec	9 Sec	Instant	Instant	Instant	Instant
4	85 Million	2¼ Hours	14 Min	1½ Min	8½ Sec	Instant	Instant
5	8 Billion	9½ Days	22½ Hours	2¼ Hours	13½ Min	1¼ Min	8 Sec
6	782 Billion	2½ Years	90 Days	9 Days	22 Hours	2 Hours	13 Min
7	75 Trillion	238 Years	24 Years	2½ Years	87 Days	8½ Days	20 Hours
8	7.2 Quadrillion	22,875 Years	2,287 Years	229 Years	23 Years	2¼ Years	83½ Days

5.5 BRUTE-FORCE ATTACK ON OUR SCHEME

In this section we will discuss the probability of cracking the password using the brute-force attack within given time interval between time t1 to ∞.

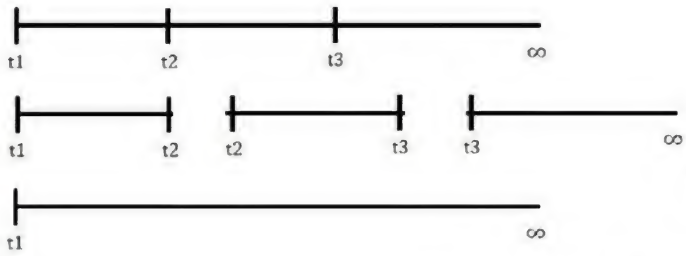


Fig 5.1: Time Sequences

1. The First parts deals between with the time between t1 to t2 for brute forcing.
2. The Second parts deals between with the time between t2 to t3 for brute forcing.
3. The third parts deals between with the time between t3 to ∞ for brute forcing.
4. And the Last Part deals between with the times between t1 to ∞ for brute forcing.

Conditions:

- If Passwords enters between the time t1 to <t2, It will be invalid even if the input password is correct or incorrect doesn't matter because time between the t1 to <t2 is equal to α and we cannot input the password with in α time.
- If password is input between the t3 to ∞ time, again it will be invalid either the input password is correct or incorrect since it will greater then μ.
- If the password enter between t1 to ∞ time, again it will be invalid even input password is correct. Since time between t1 to ∞ is greater than μ.
- If the correct password enters between t2 to <t3 along with [α, β, θ], it will be valid since the time between t2 to <t3 is equal to μ.

5.5.1 Probability Graph

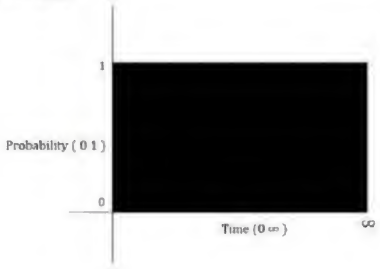


Fig 5.2: Probability Graph of brute force on previous scheme

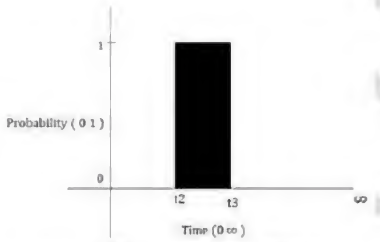


Fig 5.3: Probability Graph of brute force on our scheme.

From Fig 5.2 we can conclude that it is possible to get the password from time t1 to ∞ through brute force attack. Fig 5.3 show our scheme and it proves that brute force can only be apply on the system within time t2 to <t3. If time exceeds, system can't be access even if possible combination is found to correct because it exceeds the threshold value of μ.At the mean time only 1passwrdcombnation/per sec can be entered into the system because if more than one combination of password is entered into system for cracking it will be invalid again since for each iteration there is a timer of α sec at starting so system has to wait for α time to enter a new combination of password.

5.5.2 Time Calculation required for Brute force attack on our scheme

Let's calculate the time required to crack the password mathematically. We know that there are total 94 alpha numeric symbol keys i.e. 0123456789AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz<SP >!"#$%&'()*+,./:;<=>?@[\]^_`{|}~

We have taken the combinations of 1 to 5 digit s from the above alpha numeric symbols and characters and calculated the time requirements for brute forcing

Let the time elements be α, β, θ, δ, ψ and consider the value of this time elements ranges from 0sec to 15sec where is 15sec is threshold value .The new 5 digit password could be written as :

αAβBθCδDψE [ABCDE is 5 digit password].

For 0 sec, we will get the following combination of password.

α0A β0B θ0c δ0D ψ0E..... 1

For 1 sec, we will get the following combination

α1A β1B θ1c δ1D ψ1E..... 2

Similarly for 15 sec, we will get the following combination.

α15A β15B θ15C δ15D ψ15E..... 3

μ=It is time (in sec) in which the passwords should be entered by the user in the system otherwise authentication will be invalid.

Case 1: For 1 digit [α1A] to [α15A] and α=1 sec to 15sec respectively.

For α=1sec,

It has been observed that if the password is of one digit then there will total 94 combinations and latest super computer can break it even less than a sec.

Our scheme on 1 sec delay [α1A]: 94sec+94(Possible combination).Any computer can take up to min 94μ sec and max 188sec to crack it. i.e. 1.56 μ minutes to 3.133 μ minutes. So efficiency of our scheme is increased by 940% to 18800% just for single digit password with delay of 1 sec only. If the delay will of α =15sec i.e. [α15A] then it will take approx. 25minutes to crack it.

Case 2. For 2 digit [α1A β1B] to [α15A β15B] with α=1 sec, β=1 sec to 15sec respectively.
Total no of combinations = 3844
Latest super computer can break it even less than a sec at the speed of 10^9 password/parsec.

Our scheme for 1 sec delay: [α1A β1B]

Min :((94*1) + (94*1))*3844 μ sec=8.36 μ days.
Max :((94*1+94) + (94*1+94))*3844 μ sec=16.72 μ days

For 15 sec: [α15A β15B]

Min: ((94*15) + (94*15))*3844 μ sec=125.463 μ days
Max: ((94*15+94) + (94*15+94))*3844 μ sec=133.8281 μ

Case 3: For 5 digit [α1A β1B θ1C δ1D ψ1E] to [α15A β15B θ15C δ15D ψ15E] with α=1 sec, β=1, θ=1, δ=1, ψ=1 sec to 15sec respectively.
Total Combination: 8 Billion.
Latest Computer can break in 8 sec with the speed of 10^10passwrod/parsec.

Our Scheme for 1sec delay: [α1A β1B θ1C δ1D ψ1E]

Min: ((94*1) + (94*1) + (94*1) + (94*1) + (94*1))*8*10^9 μ sec = 119228.817859 μ year.
Max: ((94*1+94) + (94*1+94) + (94*1+94) + (94*1+94) + (94*1+94))*8*10^9 μ sec =238457.635718 μ years.

Similar for 15sec delay for in each word: [α15A β15B θ15C δ15D ψ15E].

Min: ((94*15) + (94*15) + (94*15) + (94*15) + (94*15))*8*10^9 μ sec=1788432.26788 μ years
Max: ((94*15+94) + (94*15+94) + (94*15+94) + (94*15+94) + (94*15+94))*8*10^9 μ sec=1907661.0857 μ years.

Case 4: For 8 digit [α1A β1B θ1C δ1D ψ1E Ω1# Φ1z γ1@] to [α15A β15B θ15C δ15D ψ15E Ω15# Φ15z γ15@] with α=1 sec, β=1, θ=1, δ=1, ψ=1, Ω=1, Φ=1, γ=1 sec to 15sec respectively.

Total Combination: 7.2 Quadrillion

Latest Computer can break in $83^{1/2}$ days with the speed of 10^10passwrod/parsec.

Our Scheme for 1sec delay: [α1A β1B θ1C δ1D ψ1E Ω1# Φ1z γ1@].

Min: ((94*1) + (94*1) + (94*1) + (94*1) + (94*1) + (94*1) + (94*1) + (94*1))*8*10^9 μ sec =190766.1085 μ year.

Max: ((94*1+94) + (94*1+94) + (94*1+94) + (94*1+94) + (94*1+94) + (94*1+94) + (94*1+94) + (94*1+94))*8*10^9 μ sec =381532.217μ years.

Similar for 15sec delay for in each word: [α15A β15B θ15C δ15D ψ15E Ω15# Φ15z γ15@].

Min: ((94*15) + (94*15) + (94*15) + (94*15) + (94*15+ (94*15) + (94*15) + (94*15))*8*10^9 μ sec=2861491.6286μ years

Max: ((94*15+94) + (94*15+94) + (94*15+94) + (94*15+94) + (94*15+94) + (94*15+94) + (94*15+94) + (94*15+94))*8*10^9 μ sec=3052257.7371892μ years.

Conclusion: Even for Cracking 5 Digit Password with our proposed Scheme it takes about **(17*10^5 μ)** years at the delay of 1 sec between the each digit of passwords.

Reply Attack: It is possible to capture the password in the reply attack and send back to the server after some time but again the system will not authentication the resources because in reply attack intruders can only capture the passwords but the time elements. So we can say that Reply attack on our scheme is quite impossible.

Phishing Attack: It is also not possible on our scheme. Intruders can only able get passwords but not the time elements and without the time elements authentication will be unsuccessful. Further we can say that Social Engineering is not possible our scheme.

5.5.3 Brute force attack on One Time Password of our scheme

We recommend setting a throttling specification T, which states the maximum number of possible brute force attack for One-Time Password. The remote server handle the individual table per HOTP device in order log any failed attempt. We recommend the size of T should be as low as possible. Another option can be to deploy a delay mechanism to avoid a brute force attack. Another option can be to deploy a delay mechanism to avoid a brute force attack. After each try A1, the remote server should wait for an increased T*A1 number of sec, e.g., let T = 10, and after 1 try, the remote server should waits for 6 seconds, at the second failed attempt, it waits for 10*2 = 10 seconds, etc. The delay or lockout methods must implemented across the login sessions to prevent attacks which is based on multiple parallel guessing technique.

We have proposed efficient method to get rid of brute force attack on our scheme for One Time Password. During each request of one time password a new key is generated from the table, a random table and that secrete key is use to decrypt the One Time Passwords for each login attempts or initiate the transition.Random Table produces 9X9 Matrix with 81 numbers. Each time the value of the matrix gets changes since it is random in nature .From that matrix, user needs to fetch the value (i,j) and computer the OPTy with the help of OTP which was send from the RMS and send it back to the server for the verifications. After receiving the OTPy at RMS end, RMS compare the OTPy with OTPx and return true if OTPy=OTPx. So whenever any intruders gets the OTP or able to Access the OTP he/she cannot able to produce OTPy because he/she don't know the value of i,j. Further same technique can be implemented on the Reset code too. Thus this scheme proved be a very much secure and safe in the protection of OTP at client side.

9X9 Matrix Table

Table 5.8: Random matrix table

X,Y	1	2	3	4	5	6	7	8	9
1	A1	A2	A3	A4	A5	A6	A7	A8	A9
2	A10	A11	A12	A13	A14	A15	A16	A17	A18
3	A19	A20	A21	A22	A23	A24	A25	A26	A27
4	A28	A29	A30	A31	A32	A33	A34	A35	A36
5	A37	A38	A39	A40	A41	A42	A43	A44	A45
6	A46	A47	A48	A49	A50	A51	A52	A53	A54
7	A55	A56	A57	A58	A59	A60	A61	A62	A63
8	A64	A65	A66	A67	A68	A69	**A70**	A71	A72
9	A73	A74	A75	A76	A77	A78	A79	A80	A81

The value of table get changed each time whenever the OTP request is done by user to the remote server. Let the user keys are x-7 and y-8 the respective value is (decryption key) A70 say 3. If user request new OTP the value of A70 gets changed automatically may become 9. It Proves that OTP secure at Client side. Even after shoulder attack. The Probability of getting decryption key from the table is 1/81 for each iteration.

5.5.4 Comparison of our scheme with previous scheme

Table 5.9: Comparison table

	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
Our Scheme	N	Y	Y	N	Y	Y	Y	Y	N	N
Chage-wu[21]	N	N	N	Y	Y	Y	Y	Y	Y	Y
Jan-Chen[33]	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
Yang-Shieh[32]	Y	Y	N	Y	N	N	Y	N	Y	Y
Sun[27]	N	N	N	Y	Y	Y	N	Y	Y	Y
Hwang-li[22]	N	N	N	Y	N	N	N	N	Y	Y
Liao[13]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Y: For Supported N: For Not Supported

CHAPTER 6: RESULTS AND DISCUSSION

6.1 IMPLEMENTATIONS

It is the process of deploying algorithms or decision or plan into execution or effect. We have implemented our proposed algorithms in C compiler (Dev. C and Codec Block).It's totally CUI based and we simulated our proposed scheme successfully.

Following are the Codec Block C compiler configuration details:

- For **Codec Block** Complier.

  Features

  Version: 16.01

  Cross –platform .Runs on Linux, Mac, Windows.

  Written in C++. No interpreted Languages or proprietary libs needed.

  Extensible through plugins Execution.

  Supports

  Gcc (MingW/GNU GCC

  MSVC++

  Clang

  Digital Mars

  Borland C++ 5.5

  Open Watcom

- **Very fast** custom build system (no make files needed)
- Support for **parallel builds** (utilizing your CPU's extra cores)
- Multi-target projects
- Workspaces to combine multiple projects
- Inter-project dependencies inside workspace
- Imports MSVC projects and workspaces (NOTE: assembly code not supported yet)
- Imports Dev.-C++ projects

Highlights:

- **Open Source!** GPLv3, no hidden costs.
- **Cross-platform**. Runs on Linux, Mac, Windows (uses wxWidgets).
- Written in C++. No interpreted languages or proprietary libs needed.
- Extensible through plugins

Compiler:

- **Multiple compiler support**:
  - GCC (MingW / GNU GCC)
  - MSVC++
  - clang
  - Digital Mars
  - Borland C++ 5.5
  - Open Watcom
  - ...and more
- **Very fast** custom build system (no make files needed)
- Support for **parallel builds** (utilizing your CPU's extra cores)
- Multi-target projects
- Workspaces to combine multiple projects
- Inter-project dependencies inside workspace
- Imports MSVC projects and workspaces (NOTE: assembly code not supported yet)
- Imports Dev-C++ projects

Debugger:

- Interfaces GNU GDB
- Also supports MS CDB (not fully featured)

Full breakpoints support:

  - Code breakpoints

    - Data breakpoints (read, write and read/write)
    - Breakpoint conditions (break only when an expression is true)
    - Breakpoint ignore counts (break only after certain number of hits)
- Display local function symbols and arguments
- User-defined watches (support for watching user-defined types through scripting)
- Call stack
- Disassembly
- Custom memory dump
- Switch between threads
- View CPU registers

Interface:

- Syntax highlighting, customizable and extensible
- Code folding for C, C++, FORTRAN, XML and many more files.
- Tabbed interface
- Code completion
- Class Browser
- Smart indent
- One-key swap between .h and .c/.cpp files
- Open files list for quick switching between files (optional)
- External customizable "Tools"
- To-do list management with different users

6.2 OUTPUT

The output of the scheme is divided into 2 section. 1st section deals with 4D Authentication output result and 2nd section deals with OTP authentication.

6.2.1 4D Authentication Test Output and Results

Inputs are as follow:

Table 6.1: User Input Details

Users	Details
User ID:	Abc
Password:	Xyz
α:	5 sec (Act as hold time at initials position)
μ:	15sec.(Act as the total time required to input the credentials)

Table 6.2: Output Generated by Compiler for the user

Users	Details
User ID:	Abc
Password:	Xyz
α:	5 sec (Act as hold time at initials position)
μ:	15sec. (Act as the total time required to input the credentials)
(I,j):	(7,7) Computer generated user secrete key

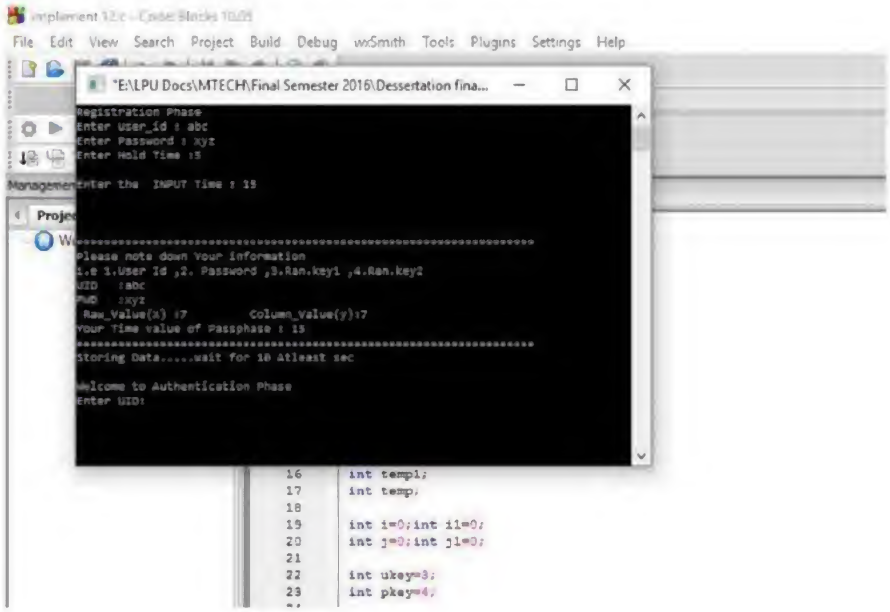


Fig 6.1: Compiler Output Screenshot

Case 1: If wrong userid and password are entered into the system

Output: **Data not matched**.

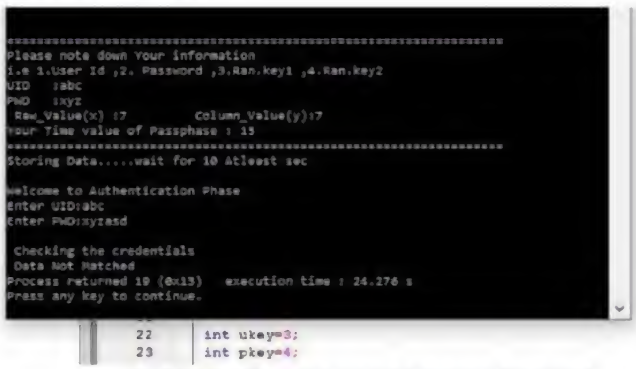


Fig 6.2: Compiler output screen if data wrong data entered

Case 2: If correct user id and password entered with in μ time but value of α exceeds.

Output: **Un-Success**

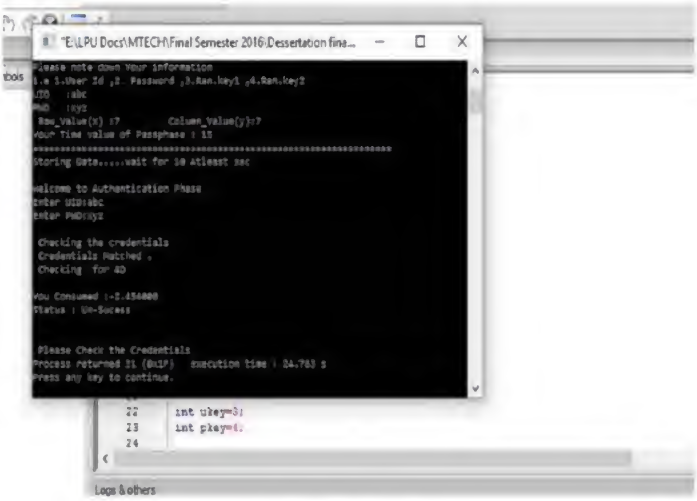


Fig 6.3: α checking

Case 3: If correct user id and password entered which exceeds μ time

Output: **Credentials Matched but 4D checking un-success.**

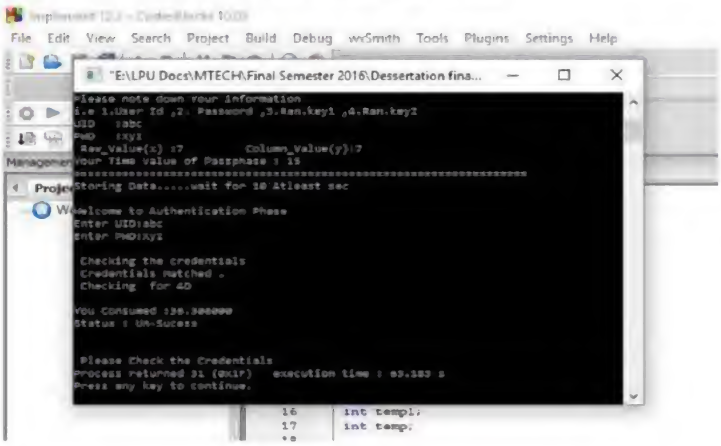


Fig 6.4: μ checking

Case 4: If correct userid and password are entered within μ time following α

Output: **4D Authentication Success and OTP (*9959*) and Random table is generated for 2nd phase of Authentication.**.

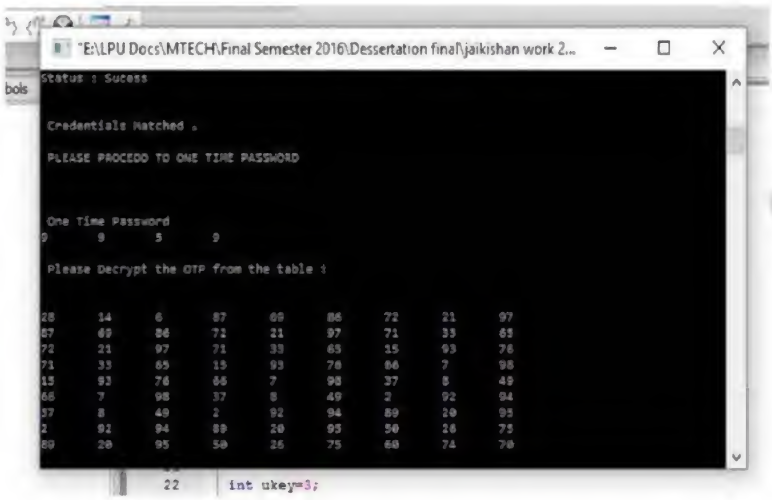


Fig 6.5: 4D Success and OTP and Random table Generated

Case 4: If Computer Generated OTP is 9959 entered.

Output: **Error Try Again**.

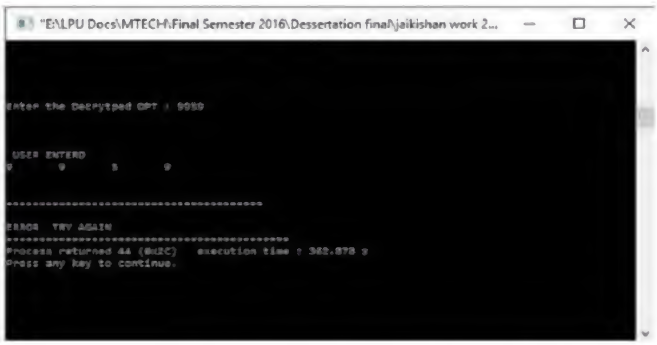


Fig 6.6: Computer Generated OTP entered

Case 5: If Decrypted OTP Entered with the key (i,j)Value i.e. 7.7 Fig[6.1],Table[6.1]

Output: **OTP Verification successful, Login Successful**

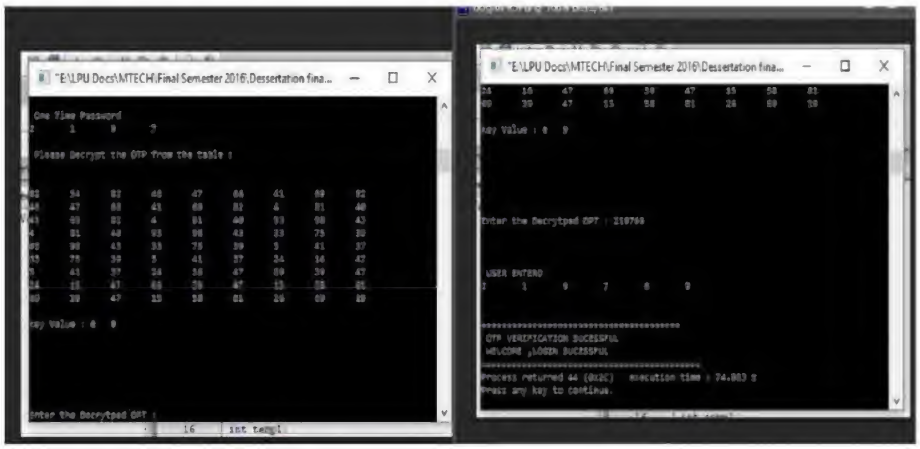


Fig 6.7: Computer Generated OTP entered

Note: Since the OTP is in dynamic Nature it gets changes in next time and it becomes 2197 and Value fetched from the table is 69 at 7, 7. OTP is decrypted with 69 and send to RMS verifications.

Case 6: Brute-Force At delay of 1 sec on 1 digit Password.

Output: **Success in but in 28sec**

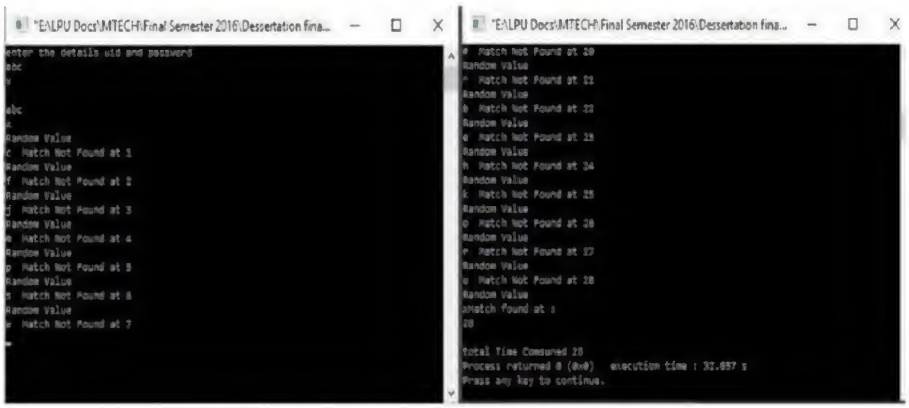


Fig 6.8: Brute Force attack on 1 digit password at 1 sec delay

Note: Even latest super computer requires min 28sec to break it. Since the CPU Processing is made limited through this Algorithms.

CHAPTER 7: CONCLUSION AND FUTURE SCOPE

7.1 CONCLUSION

In this paper, we have proposed a new 4D- authentication scheme and enhancement of OTP for database security. We have taken ten requirements for evaluating our new 4D-password authentication enchantments of OTP for database security scheme. We found that our new scheme is far better than previous one.

Following are the advantages of our new scheme.

1. User are free to choose their ids and passwords and even their passwords at will.
2. Whenever passwords gets changed, system automatically change the keys (i,j).
3. It has one time password property and it is secure at both side. Client and server side.
4. It can withstand the guessing attack, brute force attack, reply attack.
5. It can also withstand on even passwords or OTP is compromised or hacked.

7.2 FUTURE WORK

Our scheme has a lots of identifiers like time elements, secrete keys etc. By which users gets hard to memorize all the identifiers for the authentication so it adds little complexity to our proposed scheme. Future work can be done in the following ways:

1. By reducing the number of identifiers.
2. By making time elements more efficient and dynamic.
3. Scheme works on real time environments. Delay in transmission of data may result a failure.

REFERENCES

[1] Dr.AnanthiShesashaayee, D. Sumathy Associate Professor & Head, Department of Computer Science, Quaid E Millath Government College for Women, Chennai, Tamil Nadu, India Research Scholar, Department of Computer Science, Quaid E Millath Government College for Women, Chennai.Tamil Nadu, OTP Encryption Techniques in Mobile for Authentication and Transaction Security.India.IJIRCCE ISSN(2320-9801,2320-9798)-2014.

[2] Ting-Yi Chang, Cheng-Jung Tsai, and Jyun-Hao Lin. A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices. Journal of Systems and Software, 85(5):1157–1165, 2012.

[3] Brajesh Kumar Kushwaha. An approach for user authentication one time password (numeric and graphical) scheme. Journal of Global Research in Computer Science, 3(11), 2012.

[4] Nicolas Popp, David M'raihi, and Loren Hart. One time password, December 27 2011. US Patent 8,087,074.

[5] Vaidya, Binod, Park, Jong Hyuk, Yeo, Sang-Soo & Rodrigues, Joel JPC (2011). Robust one-time password authentication scheme using smart card for home network environment. Computer Communications, 34, 326-336.

[6] Jung-Sik Cho, Sang-Soo Yeo, and Sung Kwon Kim. Securing against brute-force attack: A hash-based rfid mutual authentication protocol using a secret value. Computer Communications, 34(3):391–397, 2011.

[7] M Viju Prakash, P Alwin Infant, and S Jeya Shobana. Eliminating vulnerable attacks using one time password and passtext analytical study of blended schema. Universal Journal of Computer Science and Engineering Technology, 1(2):133–140, 2010.

[8] TongLiang Li and ZhiGang Jin. A new low cost one time id and password authentication protocol using popular removable storage devices. In 2009 Second International Conference on Intelligent Networks and Intelligent Systems, pages 213–216. IEEE, 2009.

[9] Jongpil Jeong, Min Young Chung, and Hyunseung Choo, Integrated otp-based user authentication scheme using smart cards in home networks, Hawaii International Conference on System Sciences, Proceedings of the 41st Annual, IEEE, 2008, pp. 294–294.

[10] John G Brainard, Burton S Kaliski Jr, and Ronald L Rivest. Method and apparatus for performing enhanced time-based authentication, April 22 2008. US Patent 7,363,494.

[11] William Stallings and Lawrie Brown. Computer security. Principles and Practice, 2008

[12] I. You, E.S. Jung, A Light Weight Authentication Protocol for Digital Home Networks. Computational Science and Its Applications – ICCSA 2006, LNCS 3983, 2006, pp. 416–423

[13] I-En Liao, Cheng-Chi Lee, and Min-Shiang Hwang, A password authentication scheme over insecure networks, Journal of Computer and System Sciences 72 (2006), no. 4, 727–740.

[14] N.Y. Lee, J.C. Chen, Improvement of one-time password authentication scheme using smart card, IEICE Transaction on Communications E88-B (9) (2005) 3765–3769.

[15] H.S. Jo, H.Y. Youn, A Secure User Authentication Protocol Based on One-Time-Password for Home Network. Computational Science and Its Applications – ICCSA 2005, LNCS 3480, 2005, pp. 519–528

[16]] E.J. Yoon, K.Y. Yoo, More efficient and secure remote user authentication scheme with smart cards, in: Proceedings of 11th International Conference on Parallel and Distributed System, vol. 2, 2005, pp. 73–77.

[17] Blake Ross, Collin Jackson, Nick Miyake, Dan Boneh, and John C Mitchell, Stronger password authentication using browser extensions., Usenix security, Baltimore, MD, USA, 2005, pp. 17–32.

[18] James Wayman, Anil Jain, Davide Maltoni, and Dario Maio. An introduction to biometric authentication systems. Springer, 2005.

[19] Alen Peacock, Xian Ke, and Matthew Wilkerson. Typing patterns: A key to user identification. IEEE Security & Privacy, (5):40–47, 2004.

[20] Umut Uludag, Sharath Pankanti, Salil Prabhakar, and Anil K Jain. Biometric cryptosystems: issues and challenges. Proceedings of the IEEE, 92(6):948–960, 2004.

[21] Shyi-Tsong Wu and Bin-Chang Chieu, A user friendly remote authentication scheme wit smart cards, Computers & Security 22 (2003), no. 6, 547–550

[22] J.J. Shen, C.W. Lin, M.S. Hwang, Security enhancement for the time-stamp based Password authentication scheme using smart cards, Computer and Security 22 (7) (2003) 591–593

[23] Jane Zhen and Sampalli Srinivas. Preventing replay attacks for secure routing in ad hoc networks. In Ad-Hoc, Mobile, and Wireless Networks, pages 140–150. Springer, 2003.

[24] T.S. Messerges, E.A. Dabbish, R.H. Sloan, Examining smart-card security under the threat of power analysis attacks, IEEE Transactions on Computers 51 (5) (2002) 541–552.

[25] Fabian Monrose, Michael K Reiter, and Susanne Wetzel. Password hardening based on keystroke dynamics. International Journal of Information Security, 1(2):69–83, 2002.

[26] Francesco Bergadano, Daniele Gunetti, and Claudia Picardi. User authentication through keystroke dynamics. ACM Transactions on Information and System Security (TISSEC), 5(4):367–397, 2002.

[27] H.-M. Sun, An efficient remote use authentication scheme using smart cards, IEEE Trans. Consumer Electron.46 (4) (2000) 958–961

[28] M.-S. Hwang, L.-H. Li, A new remote user authentication scheme using smart cards, IEEE Trans. Consumer Electron. 46 (1) (2000) 28–30.

[29] Fabian Monrose and Aviel D Rubin. Keystroke dynamics as a biometric for authentication. Future Generation computer systems, 16(4):351–359, 2000

[30] Sajjad Haider, Ahmed Abbas, and Abbas K Zaidi. A multi-technique approach for user identification through keystroke dynamics. In Systems, Man, and Cybernetics, 2000 IEEE International Conference on, volume 2, pages 1336–1341. IEEE, 2000

[31] P. Kocher, J. Jaffe, B.B. Jun. Differential power analysis, in: Proceedings of Advances in Cryptology (CRYPTO'99), 1999, pp. 388–397.

[32] W.H. Yang, S.P. Shieh, Password authentication schemes with smart cards, Comput. Secur.18 (8) (1999)727–733.

[33] J.K. Jan, Y.Y. Chen, 'Paramita wisdom' password authentication scheme without verification tables, J. Syst.Softw. 42 (1998) 45–57.

[34] H. Krawczyk, M. Bellare, R. Canetti, HMAC: Keyed-Hashing for Message Authentication, IETF RFC 2104, February 1997.

[35] MS Obaidat and B Sadoun. Keystroke dynamics based authentication. In Biometrics, pages 213–229. Springer, 1996.

[36] H.J. Kim, Biometrics, is it a viable proposition for identity authentication and access control, Computer Secure. 14 (1995) 205–214. G.B. Purdy, A high security log-in procedure, Commun. ACM 17 (1974) 442–445.

[37] R. Joyce, G. Gupta, Identity authentication based on keystroke latencies, Commun. ACM 33 (1990) 168–176.